

# 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_42744595/article/details/122277621](https://blog.csdn.net/weixin_42744595/article/details/122277621)

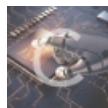
版权



取证 同时被 3 个专栏收录

5 篇文章 2 订阅

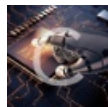
订阅专栏



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

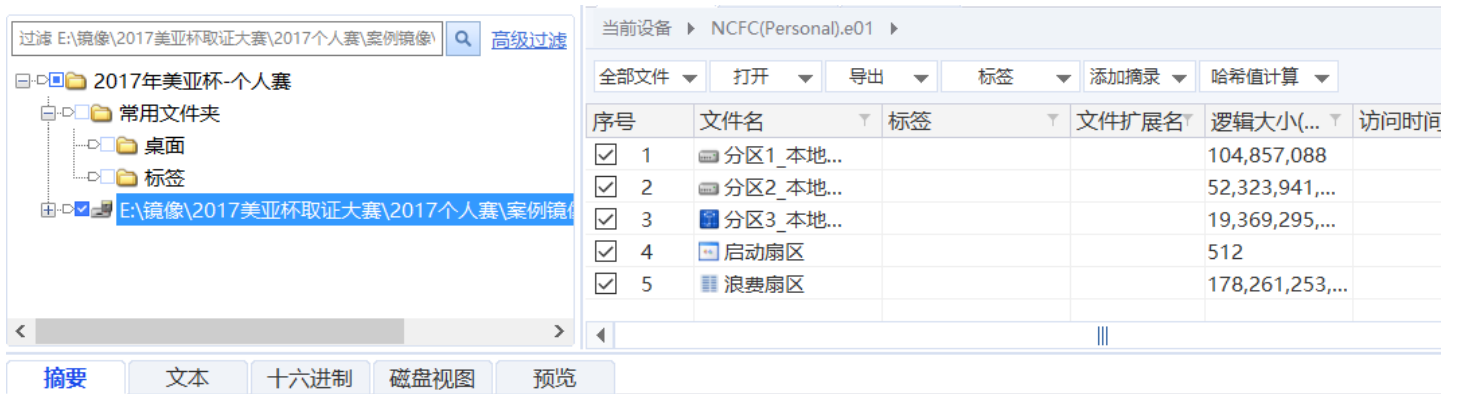
2017年美亚杯全国电子数据取证大赛

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

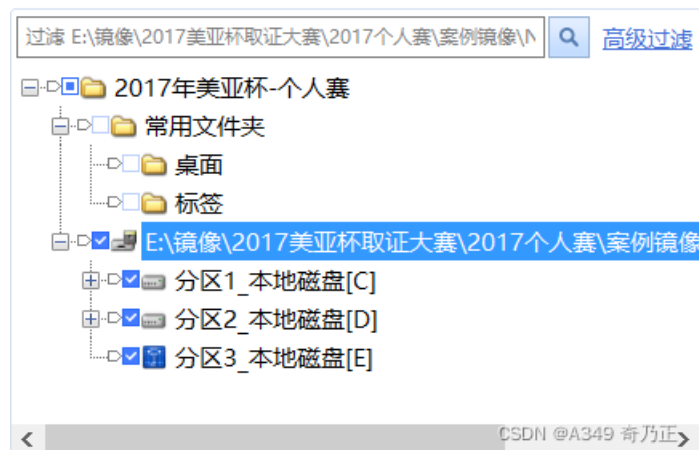
解析: 使用取证大师进行分析



CSDN @A349 奇乃正

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

名称	描述	扩展名	大小	创建时间	修改时间	记录属性	第一扇区
未分区空间	虚拟的 (检查要求)		166 GB				140,232,...
分区 3	分区, 现存的	?	18.0 GB				102,402,...
分区 2	分区, 现存的	NTFS	48.7 GB				206,848
分区 1	分区, 现存的	NTFS	100 MB				2,048
起始扇区	虚拟的 (检查要求)		1.0 MB				0

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=?

00000190	0E 07 00 00 00 00 74 03	0D 00 4D 03 73 73 03 0E	ny
000001A0	67 20 6F 70 65 72 61 74	69 6E 67 20 73 79 73 74	g ope
000001B0	65 6D 00 00 00 63 7B 00	7D 84 0F 52 DA 3D 80 20	em
000001C0	21 00 07 DF 13 0C 00 08	00 00 00 20 03 00 00 DF	! B
000001D0	14 0C 07 FE FF FF 00 28	03 00 00 60 17 06 00 FE	þj
000001E0	FF FF 07 FE FF FF 00 88	1A 06 00 40 41 02 00 00	ÿþ
000001F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 55 AA	
00000200	70 6C 55 36 4A DC B3 E0	13 CE 00 00 00 00 00 00	þU6.
00000210	4F F5 44 A9 FC 4B BF AB	8E 01 00 00 00 00 00 00	þ OðD@i
00000220	A0 B3 5D B8 68 E4 A3 25	11 72 00 00 00 00 00 00	þC ð],þ
00000230	1F 92 3D F9 43 81 57 25	AD A9 00 00 00 00 00 00	þ0 '=ùC
00000240	50 DE 1E F1 DB 20 F2 6A	51 1F 00 00 00 00 00 00	þF ð-ñC

数据解释器

8 Bit (±): 0

16 Bit (±): 24 576

32 Bit (±): 102 195 200

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

18.7 SR-2 x64

硬盘 2 硬盘 2, 分区 2

3 分钟前 15+0+4=19 文件, 15+0+1=16 目录

名称	描述	扩展名	大小	创建时间	修改时间	记录属性	第一扇区
SWSetup	现存的		336 B	2017/0...	2017/...	201...	6,326,412
System Volume Information	现存的		4.1 KB	2017/0...	2017/...	201...	11,411,5...
tmp	现存的		152 B	2017/1...	2017/...	201...	6,382,824
Users	现存的		4.1 KB	2009/0...	2017/...	201... R	976,208
Windows	现存的		16.4 KB	2009/0...	2017/...	201...	3,328
\$AttrDef	现存的		2.5 KB	2017/0...	2017/...	201... SH	6,157,768
\$BadClus	现存的		0 B	2017/0...	2017/...	201... SH	6,291,472
\$Bitmap	现存的		1.5 MB	2017/0...	2017/...	201... SH	6,288,320
\$Boot	现存的		8.0 KB	2017/0...	2017/...	201... SH	0
\$LogFile	现存的		64.0 MB	2017/0...	2017/...	201... SH	6,026,176
\$MFT	现存的		118 MB	2017/0...	2017/...	201... SH	6,291,456
\$MFTMirr	现存的		4.0 KB	2017/0...	2017/...	201... SH	16

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	FILE	is N
0C000000	46	49	4C	45	30	00	03	00	EC	73	03	4E	00	00	00	00	FILE	is N
0C000010	01	00	01	00	38	00	01	00	B8	01	00	00	00	04	00	00	8	,
0C000020	00	00	00	00	00	00	00	00	06	00	00	00	00	00	00	00	n	
0C000030	6E	00	86	87	00	00	00	00	10	00	00	00	60	00	00	00		,
0C000040	00	00	18	00	00	00	00	00	48	00	00	00	18	00	00	00		H
0C000050	28	65	C2	49	64	25	D3	01	28	65	C2	49	64	25	D3	01	(eÅId%Ó	(eÅId%Ó
0C000060	28	65	C2	49	64	25	D3	01	28	65	C2	49	64	25	D3	01	(eÅId%Ó	(eÅId%Ó
0C000070	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		,
0C000080	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00		,
0C000090	00	00	00	00	00	00	00	00	30	00	00	00	68	00	00	00		0 h
0C0000A0	00	00	18	00	00	00	03	00	4A	00	00	00	18	00	01	00		J
0C0000B0	05	00	00	00	00	00	05	00	28	65	C2	49	64	25	D3	01		(eÅId%Ó
0C0000C0	28	65	C2	49	64	25	D3	01	28	65	C2	49	64	25	D3	01		(eÅId%Ó (eÅId%Ó

扇区 6,291,456 102,195,200 偏移量: C0000000 = 70 选块: 不可用

硬盘 2, 分区 2 58% 空余  
文件系统: NTFS  
缺省编辑模式  
状态: 原始  
撤销级别: 0  
反向撤销: 不可用  
可见驱动器空间分配:  
簇号: 786,432 \$MFT (#0)  
卷快照获取于: 3 分钟前  
逻辑扇区号: 6,291,456  
物理扇区号: 6,498,304

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 —“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

自动取证(182340)

E:\镜像\2017美亚杯取证大赛\2017个人赛\案例镜... 系统痕迹(1385)

- 系统信息(581)
  - 无线上网(70)
  - 帐户登录(62)
  - 系统开机时间(81)
  - 系统信息(18)
  - 用户信息(7)
  - 服务信息(148)
  - 硬件信息(153)
  - 网络配置(32)
  - 时区信息(1)
  - 帐户策略(9)
- 安装软件(154)
- USB设备使用痕迹(24)

导出	加入摘要	跳转到源...	打开关联...		
序号	名称	值	系统	删除状态	
<input type="checkbox"/>	1	完整计算机名	Gary-PC	Windows 7 Home Premium	正常
<input type="checkbox"/>	2	工作组	WORKGROUP	Windows 7 Home Premium	正常
<input type="checkbox"/>	3	计算机描述	Windows 7 Home Premium	Windows 7 Home Premium	正常
<input checked="" type="checkbox"/>	4	安装时间	2017-09-04 18:11:10	Windows 7 Home Premium	正常
<input type="checkbox"/>	5	产品名称	Windows 7 Home Premium	Windows 7 Home Premium	正常
<input type="checkbox"/>	6	注册组织	Windows 7 Home Premium	Windows 7 Home Premium	正常
<input type="checkbox"/>	7	注册所有者	Gary	Windows 7 Home Premium	正常
<input type="checkbox"/>	8	当前版本	6.1	Windows 7 Home Premium	正常
<input type="checkbox"/>	9	当前Build版本	7601	Windows 7 Home Premium	正常
<input type="checkbox"/>	10	最新服务包	Service Pack 1	Windows 7 Home Premium	正常
<input type="checkbox"/>	11	系统根路径	C:\Windows	Windows 7 Home Premium	正常
<input type="checkbox"/>	12	源路径	Windows 7 Home Premium	Windows 7 Home Premium	正常
<input type="checkbox"/>	13	路径名	C:\Windows	Windows 7 Home Premium	正常
<input type="checkbox"/>	14	产品ID	00359-112-0000007-85269	Windows 7 Home Premium	正常

CSDN @A349 奇乃正

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

序号	用户名	用户全称	用户类型	用户标识(SID)	用户目录	上次登录时间	登录次数	上次登录失败
1	Administra...		本地用户	S-1-5-21-58984532-3717197446-1900145663-500		2010-11-21 05:48...	6	
2	Guest		本地用户	S-1-5-21-58984532-3717197446-1900145663-501			0	
3	Gary		本地用户	S-1-5-21-58984532-3717197446-1900145663-1000	C:\Users\Gary	2017-10-31 11:53...	60	2017-10-31
4	彼得	彼得	本地用户	S-1-5-21-58984532-3717197446-1900145663-1001	C:\Users\彼得	2017-10-06 10:49...	2	2017-10-06
5			系统服务	S-1-5-18	%systemroot%\system32\config\sys...			
6			系统服务	S-1-5-19	C:\Windows\ServiceProfiles\LocalServ...			
7			系统服务	S-1-5-20	C:\Windows\ServiceProfiles\Network...			

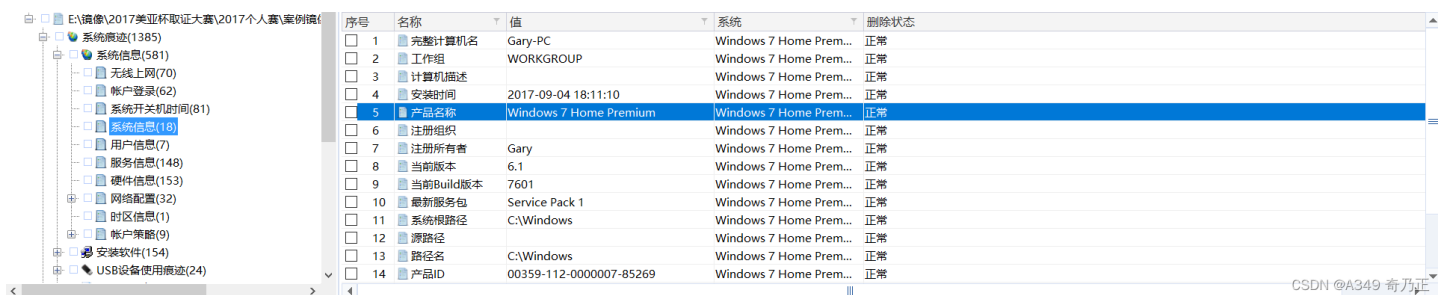
	8	用户“彼得”的SID是什么？
√	B.	1001
	A.	1000
	C.	1002
	D.	1005
	E.	1007

解析：使用取证大师进行分析

序号	用户名	用户全称	用户类型	用户标识(SID)	用户目录	上次登录时间	登录次数	上次登录失败
1	Administra...		本地用户	S-1-5-21-58984532-3717197446-1900145663-500		2010-11-21 05:48...	6	
2	Guest		本地用户	S-1-5-21-58984532-3717197446-1900145663-501			0	
3	Gary		本地用户	S-1-5-21-58984532-3717197446-1900145663-1000	C:\Users\Gary	2017-10-31 11:53...	60	2017-10-31
4	彼得	彼得	本地用户	S-1-5-21-58984532-3717197446-1900145663-1001	C:\Users\彼得	2017-10-06 10:49...	2	2017-10-06
5			系统服务	S-1-5-18	%systemroot%\system32\config\sys...			
6			系统服务	S-1-5-19	C:\Windows\ServiceProfiles\LocalServ...			
7			系统服务	S-1-5-20	C:\Windows\ServiceProfiles\Network...			

	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.	<a href="http://www1.10086.com">www1.10086.com</a>

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.	<a href="http://www.188bet.com">www.188bet.com</a>	
c.	<a href="http://www.hv5858.com">www.hv5858.com</a>	
d.	<a href="http://www.12377.cn">www.12377.cn</a>	
e.	<a href="http://www.88.bettingwell.com">www.88.bettingwell.com</a>	
f.	<a href="http://www.aaakk.org">www.aaakk.org</a>	
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

www.188bet.com

搜索结果(116)

- E:\2017个人赛\案例镜像\NCFC(Persona
- 文件分析(2)
- 上网记录(111)
  - Google Chrome(111)
    - Google Chrome缓存记录(72)
    - Google Chrome历史记录(37)
    - Google Chrome Cookies(1)
    - Google Chrome登录信息(1)
  - 证据文件(3)

序号	解码后的URL	标题
1	<a href="https://www.188bet.com/zh-cn/?affili...">https://www.188bet.com/zh-cn/?affili...</a>	188BET_亚洲体育博彩及真人娱...
2	<a href="https://www.188bet.com/zh-cn?affilia...">https://www.188bet.com/zh-cn?affilia...</a>	188BET_亚洲体育博彩及真人娱...
3	<a href="https://www.188bet.com/zh-cn">https://www.188bet.com/zh-cn</a>	188BET_亚洲体育博彩及真人娱...
4	<a href="https://www.188bet.com/zh-cn">https://www.188bet.com/zh-cn</a>	188BET_亚洲体育博彩及真人娱...
5	<a href="https://www.188bet.com/zh-cn/sport...">https://www.188bet.com/zh-cn/sport...</a>	188BET体育博彩_立即进行选择您...
6	<a href="https://www.188bet.com/zh-cn/sport...">https://www.188bet.com/zh-cn/sport...</a>	188BET体育博彩_立即进行选择您...
7	<a href="https://www.188bet.com/zh-cn/sport...">https://www.188bet.com/zh-cn/sport...</a>	188BET体育博彩_立即进行选择您...
8	<a href="https://www.188bet.com/zh-cn/sign-up">https://www.188bet.com/zh-cn/sign-up</a>	
9	<a href="https://www.188bet.com/postlogin">https://www.188bet.com/postlogin</a>	
10	<a href="https://www.188bet.com/zh-cn/sign-...">https://www.188bet.com/zh-cn/sign-...</a>	
11	<a href="https://www.188bet.com/zh-cn/my-ac...">https://www.188bet.com/zh-cn/my-ac...</a>	
12	<a href="https://www.188bet.com/zh-cn">https://www.188bet.com/zh-cn</a>	188BET_亚洲体育博彩及真人娱...
13	<a href="https://www.188bet.com/zh-cn">https://www.188bet.com/zh-cn</a>	188BET_亚洲体育博彩及真人娱...
14	<a href="https://www.188bet.com/zh-cn">https://www.188bet.com/zh-cn</a>	188BET_亚洲体育博彩及真人娱...
15	<a href="https://www.188bet.com/zh-cn/sports">https://www.188bet.com/zh-cn/sports</a>	188BET体育博彩_立即进行选择您...
16	<a href="https://www.188bet.com/zh-cn/lotto">https://www.188bet.com/zh-cn/lotto</a>	188BET彩票_享受13种高频率彩...
17	<a href="https://www.188bet.com/zh-cn/lotto/l...">https://www.188bet.com/zh-cn/lotto/l...</a>	188BET彩票_享受13种高频率彩...
18	<a href="https://www.188bet.com/zh-cn/anno...">https://www.188bet.com/zh-cn/anno...</a>	
19	<a href="https://www.188bet.com/zh-cn/anno...">https://www.188bet.com/zh-cn/anno...</a>	
20	<a href="https://www.188bet.com/zh-cn/my-ac...">https://www.188bet.com/zh-cn/my-ac...</a>	
21	<a href="https://www.188bet.com/zh-cn/bingo">https://www.188bet.com/zh-cn/bingo</a>	188BET彩票_Bingo_现在开始体验...

www.88.bettingwell.com

搜索结果(84)

- E:\2017个人赛\案例镜像\NCFC(Persona
- 上网记录(84)
  - Google Chrome(84)
    - Google Chrome缓存记录(72)
    - Google Chrome历史记录(11)
    - Google Chrome Cookies(1)

序号	解码后的URL	标题
1	<a href="http://www.88.bettingwell.com/tiyu-b...">http://www.88.bettingwell.com/tiyu-b...</a>	博彩及博彩分析
2	<a href="http://www.88.bettingwell.com/tiyu-b...">http://www.88.bettingwell.com/tiyu-b...</a>	
3	<a href="http://www.88.bettingwell.com/zhidet...">http://www.88.bettingwell.com/zhidet...</a>	在线博彩公司和博彩公司评论。最...
4	<a href="http://www.88.bettingwell.com/tiyu-b...">http://www.88.bettingwell.com/tiyu-b...</a>	不对玩家进行限制的博彩公司。...
5	<a href="http://www.88.bettingwell.com/tiyu-b...">http://www.88.bettingwell.com/tiyu-b...</a>	在线体育投注
6	<a href="http://www.88.bettingwell.com/tiyu-b...">http://www.88.bettingwell.com/tiyu-b...</a>	体育博彩数学
7	<a href="http://www.88.bettingwell.com/tiyu-b...">http://www.88.bettingwell.com/tiyu-b...</a>	覆盖投注
8	<a href="http://www.88.bettingwell.com/tiyu-b...">http://www.88.bettingwell.com/tiyu-b...</a>	覆盖投注
9	<a href="http://www.88.bettingwell.com/">http://www.88.bettingwell.com/</a>	在线博彩公司和体育博彩门户网站...
10	<a href="http://www.88.bettingwell.com/bocai...">http://www.88.bettingwell.com/bocai...</a>	体育博彩新闻和体育赛事分析
11	<a href="http://www.88.bettingwell.com/bocai...">http://www.88.bettingwell.com/bocai...</a>	缓存资金



	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。

序号	URL地址	登录名称	访问次数	删除状态
1	https://www.188bet.com/zh-cn/sign-up	garychen88	1	正常

	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。

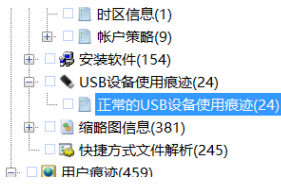
再在注册表里仔细查找发现这五个设备好像都有，这道题我感觉没有正确答案

- USBSTOR
- CdRom&Ven\_BUFFALO&Prod\_Optical\_Drive&Rev\_1.00
- Disk&Ven\_General&Prod\_UDisk&Rev\_5.00
- Disk&Ven\_Generic&Prod\_Flash\_Disk&Rev\_8.07
- Disk&Ven\_Samsung&Prod\_Portable\_SSD\_T1&Rev\_0
- Disk&Ven\_StoreJet&Prod\_Transcend&Rev\_0
- Disk&Ven\_StoreJet&Prod\_TS256GESD400K&Rev\_0
- Disk&Ven\_WD&Prod\_My\_Passport\_0827&Rev\_1012
- Other&Ven\_WD&Prod\_SES\_Device&Rev\_1012

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

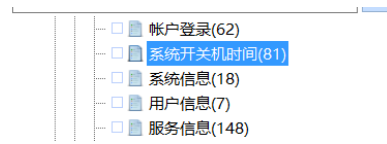
解析：同上题



<input type="checkbox"/>	3	0000.001d.0000.001.007.000.000.000.000		
<input type="checkbox"/>	4	BUFFALO Optical Drive USB Device	CdRom&Ven_BUFFALO&Prod_Optical_Drive&Rev_1.00	
<input checked="" type="checkbox"/>	5	General UDisk USB Device	Disk&Ven_General&Prod_UDisk&Rev_5.00	Z:
<input type="checkbox"/>	6	General UDisk USB Device	Disk&Ven_General&Prod_UDisk&Rev_5.00	
<input type="checkbox"/>	7	General UDisk USB Device	Disk&Ven_General&Prod_UDisk&Rev_5.00	
<input type="checkbox"/>	8	Generic Flash Disk USB Device	Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07	F:
<input type="checkbox"/>	9	Port_#0001.Hub_#0001		
<input type="checkbox"/>	10	Port_#0001.Hub_#0001		

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	

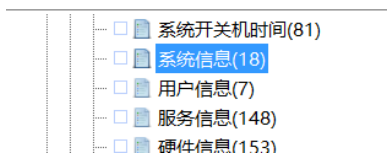
关机时间：2017-10-31 11:47:36



序号	开机时间	关机时间	持续时间	备注	删除状态
<input checked="" type="checkbox"/>	2017-10-31 11:44:04	2017-10-31 11:47:36	0:00:03:32	系统即将进入...	正常
<input type="checkbox"/>	2017-10-30 17:34:12	2017-10-30 18:03:56	0:00:29:44	系统即将进入...	正常
<input type="checkbox"/>	2017-10-30 17:15:25	2017-10-30 17:19:17	0:00:03:52	系统即将进入...	正常

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	

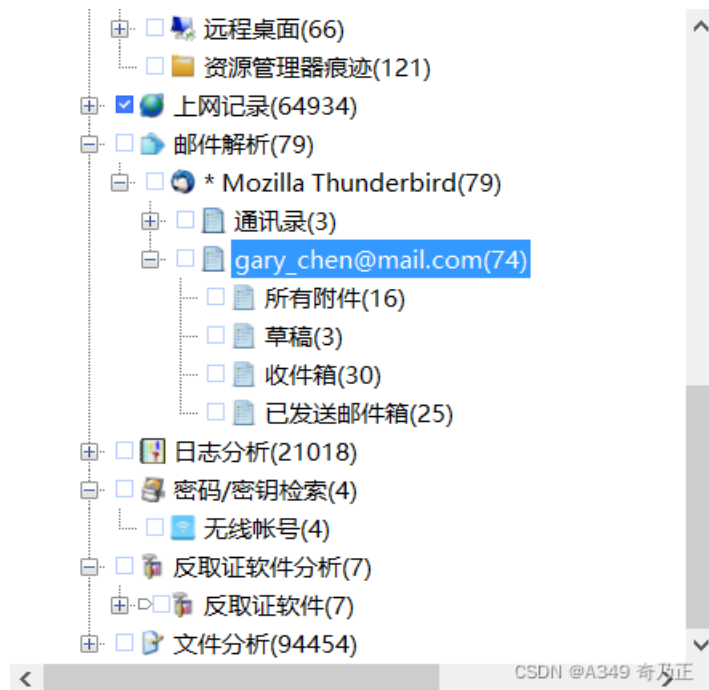
解析：在取证大师中系统信息项直接可见。



序号	名称	值	系统	删除状态
<input checked="" type="checkbox"/>	完整计算机名	Gary-PC	Windows 7 Home Prem...	正常
<input type="checkbox"/>	工作组	WORKGROUP	Windows 7 Home Prem...	正常
<input type="checkbox"/>	计算机描述		Windows 7 Home Prem...	正常

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 <b>ics_user@mail.com</b> 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

发件人: ICS USER<ics\_user@mail.com>  
 收件人: gary\_chen<gary\_chen@mail.com>;  
 邮件主题: 你需要的信息  
 内容: Gary,

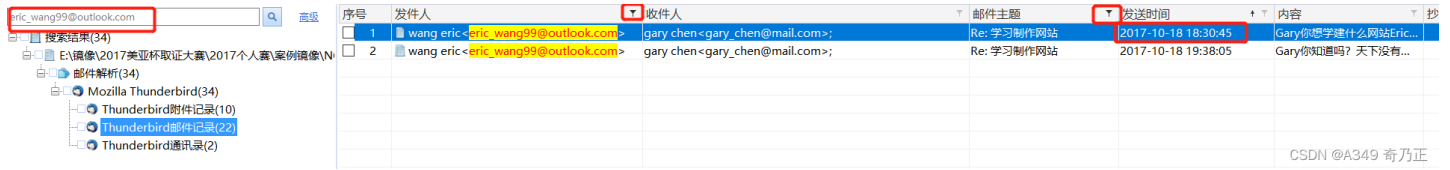
哈哈，其实我也不是真正的专家，我也是跟其他人学的，我给你他的email吧，如果你真的有兴趣，你可以email给他，看看他会不会回覆你，他的email是eric\_wang99@outlook.com.

发送时间: 2017-10-17 18:24:02  
 服务器接收时间: 2017-10-17 18:24:02  
 附件个数: 0  
 邮件中转IP: 210.3.92.18; 74.208.4.200; 74.208.5.20  
 删除状态: 正常

20	在该Windows系统中，用户Gary还曾经收过两封来自邮箱帐号 <b>eric_wang99@outlook.com</b> 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？
----	---

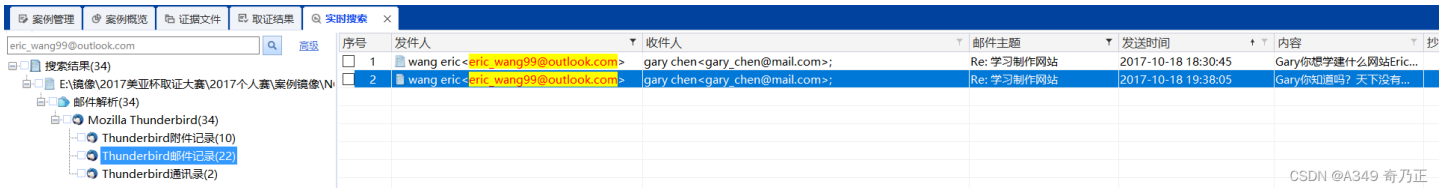
20	在该Windows系统中，用户Gary还曾经收过两封来自邮箱帐号 <b>eric_wang99@outlook.com</b> 的邮件，标题为“学习制作网站”，下列哪个是第一封邮件的发送日期和时间？
A.	2017-09-25 17:07:15
B.	2017-10-17 14:35:45
C.	2017-10-17 18:24:02
√ D.	2017-10-18 18:30:45
E.	2017-10-18 19:38:05

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。



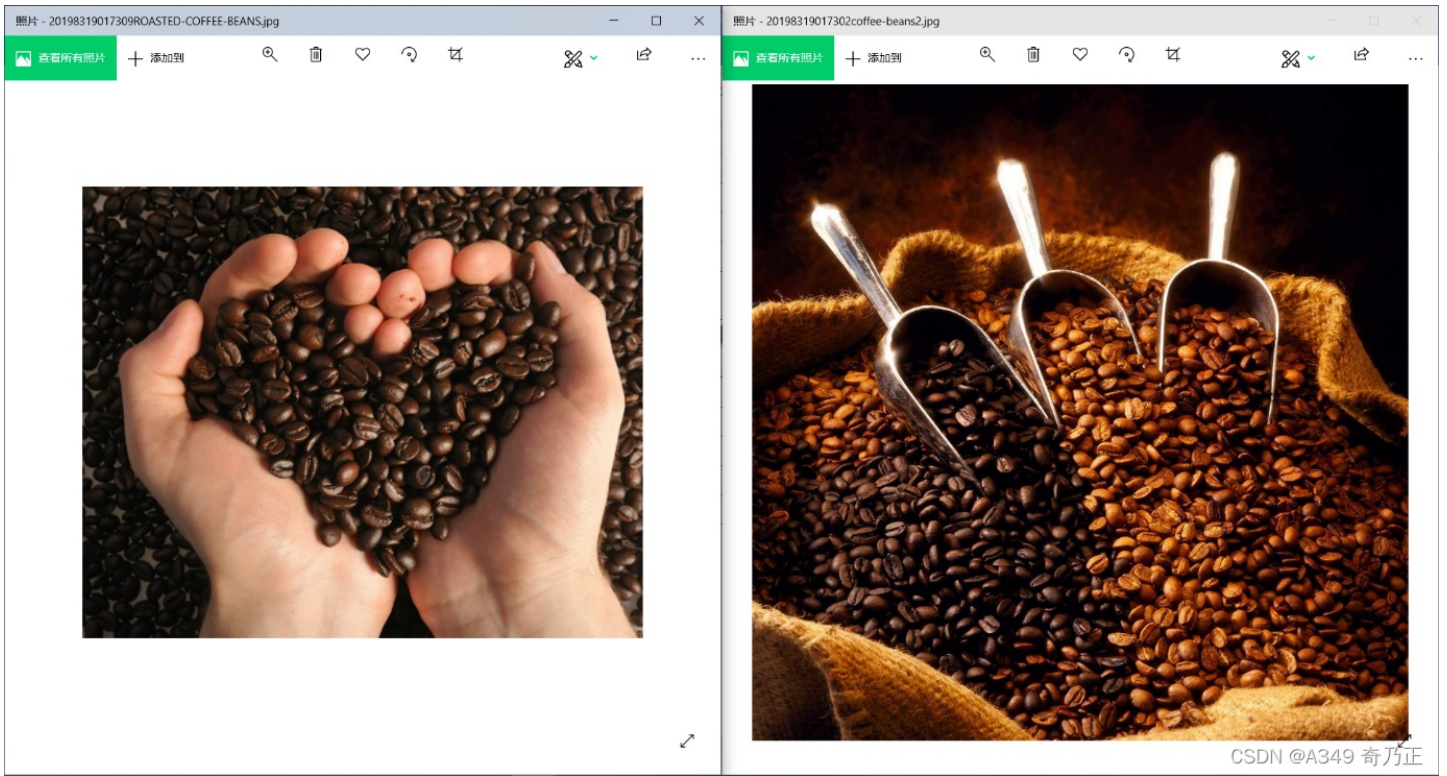
21	在该Windows系统中，用户Gary还曾经收过两封来自邮箱帐号 <b>eric_wang99@outlook.com</b> 邮件，标题为“学习制作网站”，下列哪个是第二封电邮的发送日期和时间？
A.	2017-09-25 17:07:15
B.	2017-10-17 14:35:45
C.	2017-10-17 18:24:02
D.	2017-10-18 18:30:45
√ E.	2017-10-18 19:38:05

解析：方法同上题。



22	用户Gary还曾经收过一封来自邮箱帐号 <b>ics_user@mail.com</b> 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

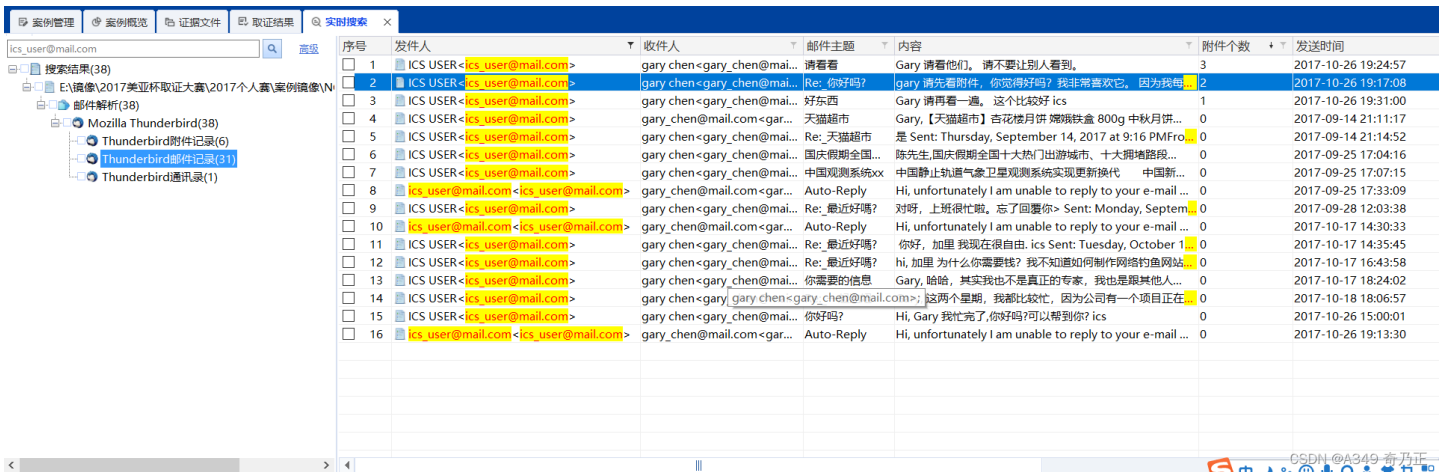
解析：在取证大师中以“ics\_user@mail.com”为关键词实时搜索，在邮件解析-邮件记录项中对发件人和附件个数进行过滤，可得答案



CSDN @A349 奇乃正

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

CSDN @A349 奇乃正



CSDN @A349 奇乃正

23	下列哪项是与上述咖啡豆有关相片的MD5哈希值/哈希值(Hash value)?
A.	449cebf0eb96499df047fe0bff8e1627
√ B.	17f9c6bcc44d128f7ed6769a6920278
C.	4bc48ce355acd4732f33a79e29728e96
D.	4bc48ce355acd4732f33a79e29728e96



23	下列哪项是与上述咖啡豆有关相片的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 <a href="mailto:eric_wang99@outlook.com">eric_wang99@outlook.com</a> 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

序号	发件人	收件人	邮件主题	内容	附件个数	抄送
1	wang eric <eric_wang99@outlook.com>	gary chen <gary...>	Re: 学习制作网站	Gary你知道吗？天下没有免费的午餐，如果你真的想学建站网站，我可以教你...	3	
2	wang eric <eric_wang99@outlook.com>	gary chen <gary...>	连结	Gary你说你连不到的连结，我可以连到，请看下面三张照片。是你想要买吗？ Eric	3	
3	wang eric <eric_wang99@outlook.com>	gary chen <gary...>	连结	Gary你说你连不到的连结，我可以连到，请看下面三张照片。是你想要买吗？ Eric	3	
4	wang eric <eric_wang99@outlook.com>	gary chen <gary...>	网站价钱	GaryCloud 网站源代码的价钱要一千块钱，买手枪或刀就有一点难说，这样吧，...	1	
5	wang eric <eric_wang99@outlook.com>	gary chen <gary...>	Re: 学习制作网站	Gary你想学建什么网站EricOn 2017/10/18 18:15, gary chen wrote:> Eric,> >...	0	
6	wang eric <eric_wang99@outlook.com>	gary chen <gary...>	Re: 连结	Gary你要看多少时间？你不想买，对吧？ EricOn 2017/10/27 18:46, gary che... 0		
7	wang eric <eric_wang99@outlook.com>	gary chen <gary...>	Re: 确认买买买	Gary给你一个网盘，自己去看看http://mantech.mooco.com:8000登录名: dunc... 0		
8	wang eric <eric_wang99@outlook.com>	gary chen <gary...>	发票	Gary发票已在私人云端发送给您，您可以在私人云下载发票,发票名称: invoice.zi... 0		

序号	附件名	附件路径	附件大小(字节)
1	icloud1.png	C:\Program Files\取证大师\FMP\Case\2017年美亚杯-个人赛\Report\45368AA272C8452aA30CF40F9A7F39D1\Attachment\13572\0\0\20198319017235icloud1.png	265083
2	icloud2.png	C:\Program Files\取证大师\FMP\Case\2017年美亚杯-个人赛\Report\45368AA272C8452aA30CF40F9A7F39D1\Attachment\13572\0\0\20198319017245icloud2.png	54090
3	icloud3.png	C:\Program Files\取证大师\FMP\Case\2017年美亚杯-个人赛\Report\45368AA272C8452aA30CF40F9A7F39D1\Attachment\13572\0\0\20198319017249icloud3.png	58594

附件个数：3

发送时间：2017-10-18 19:38:05

服务器接收时间：2017-10-18 19:38:10

邮件中转IP：10.152.248.172；10.152.248.58；10.152.249.95；15.20.77.10；40.92.255.22；74.208.5.22

删除状态：正常

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

导出	加入摘要	跳转到源...	打开关联...			
序号	配置名称	网络名称(SSID)	首次连接时间	最后连接时间	DNS	
<input type="checkbox"/>	1	Gary_home_2.4G	Gary_home_2.4G	2017-10-30 16:48...	2017-10-31 12:06...	<无>
<input type="checkbox"/>	2	ASUS	ASUS	2017-10-17 14:27...	2017-10-17 18:16...	<无>
<input type="checkbox"/>	3	siuloen@Xper...	siuloen@Xperia C...	2017-10-30 11:56...	2017-10-30 15:08...	<无>
<input type="checkbox"/>	4	Starbucks_Free...	Starbucks_Free_Wifi	2017-10-18 17:49...	2017-10-20 18:07...	<无>

CSDN @A349 奇乃正

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。

导出	加入摘要	跳转到源...	打开关联...					
序号	配置名称	网络名称(SSID)	首次连接时间	最后连接时间	DNS	默认网关MAC	连接类型	网络GUID
<input type="checkbox"/>	1	Gary_home_2.4G	2017-10-30 16:48...	2017-10-31 12:06...	<无>	2C-30-33-FA-43-00	ESS	{558B94DF-8D68-4779-AA25-65FBDAB4C2B9}
<input type="checkbox"/>	2	ASUS	2017-10-17 14:27...	2017-10-17 18:16...	<无>	AC-9E-17-EA-FE-F0	ESS	{8039D237-A346-4BA1-9B78-5752580ED7F0}
<input type="checkbox"/>	3	siuloen@Xperia C5 Ultra	2017-10-30 11:56...	2017-10-30 15:08...	<无>	5A-48-22-D2-26-37	ESS	{97C69DD6-ECE9-41A5-B840-D01B1848296D}
<input checked="" type="checkbox"/>	4	Starbucks_Free_Wifi	2017-10-18 17:49...	2017-10-20 18:07...	<无>	2C-30-33-FA-43-00	ESS	{AF0778E8-6C4F-41C6-84B2-CB14490CF29E}

CSDN @A349 奇乃正

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DHCP地址。

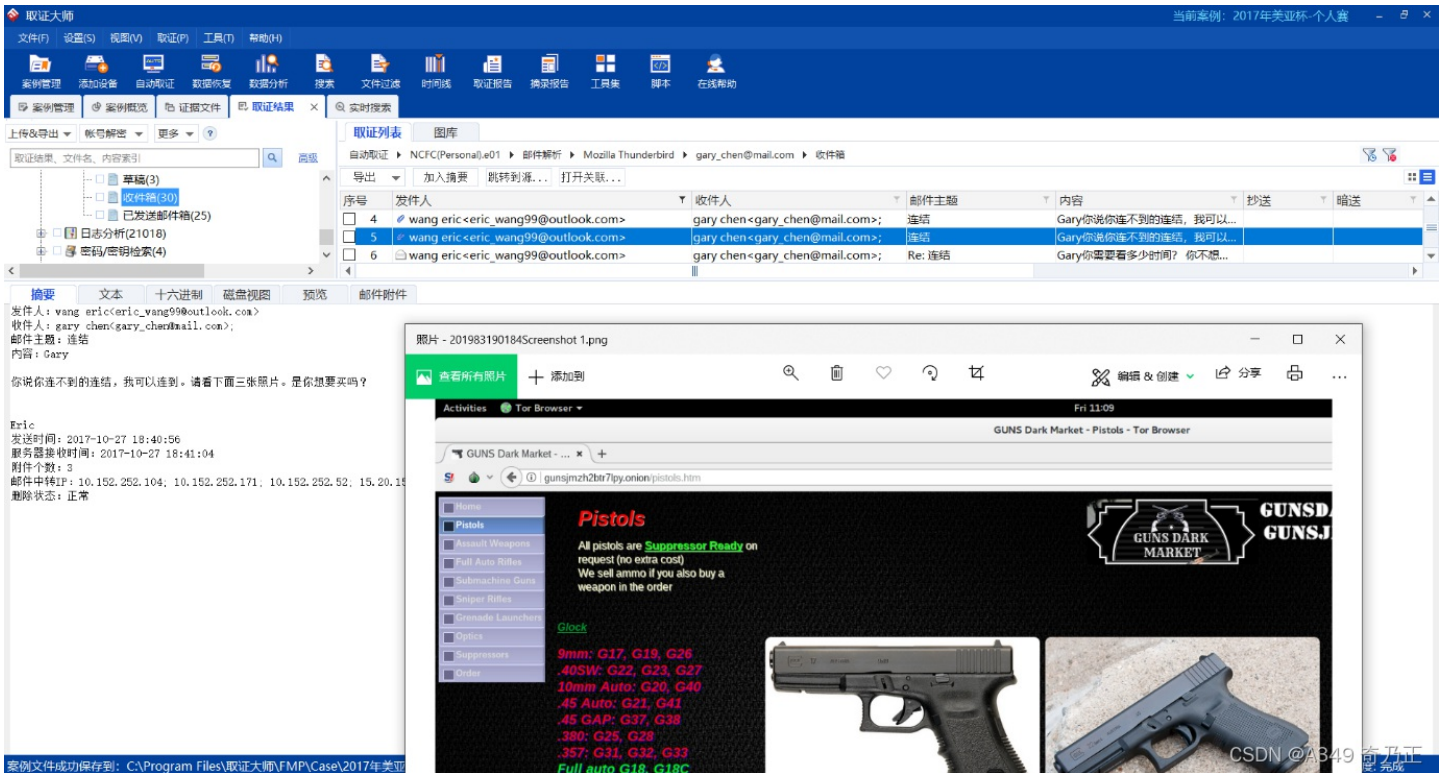
序号	MAC地址	IP地址	子网掩码	默认网关	网络名称	DHCP地址	租期获得日期	DHCP服务器	描述
1	34-DE-1A-8F-58-5E			192.168.30.1	无线网络连接	192.168.30.3	2017-10-31 12:06:26	192.168.30.1	Intel(R) Dual Band Wireless-AC 3...
2	FC-3F-D8-FB-11-36			192.168.1.2	本地连接* 11	192.168.1.94	192.168.30.3	10-30 11:39:50	Intel(R) Ethernet Connection (3) I...
3	BA-B8-20-52-41-53				本地连接* 11				WAN Miniport (IPv6)
4	00-00-00-00-00-00				isatap.{8E249539-2...				Microsoft ISATAP Adapter #3
5	20-41-53-59-4E-FF				本地连接* 10				RAS Async Adapter
6	00-00-00-00-00-00				本地连接* 9				WAN Miniport (SSTP)
7	00-00-00-00-00-00				isatap.{4863E28F-8B0...				Microsoft ISATAP Adapter
8	00-00-00-00-00-00				本地连接* 6				WAN Miniport (IKEv2)
9	00-00-00-00-00-00				本地连接* 5				WAN Miniport (PPPOE)
10	00-00-00-00-00-00				本地连接* 4				WAN Miniport (PPTP)
11	00-00-00-00-00-00				isatap.{595A8CCB-E...				Microsoft ISATAP Adapter #2
12	00-00-00-00-00-00				本地连接* 2				Bluetooth 设备(RFCOMM 协议 TD...
13	34-DE-1A-8F-58-5E				Bluetooth 网络连接	0.0.0.0		255.255.255.255	Bluetooth 设备(RFCOMM 协议 TD...

CSDN @A349 奇乃正



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://gunsdtk58tolcrrre.onion
D.	http://armoryohajjhou6m.onion
E.	http://armory45jjdf7d.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。

The screenshot shows the Mozilla Thunderbird interface. On the left, the folder tree includes '收件箱(30)' (Inbox) and '已发送邮件箱(25)' (Sent). The main pane displays an email list with the following details:

发件人	收件人	邮件主题
wang eric <eric_wang99@outlook.com>	gary chen <gary_chen@mail.com>;	Re: 学习制作网站
wang eric <eric_wang99@outlook.com>	gary chen <gary_chen@mail.com>;	Re: 学习制作网站
wang eric <eric_wang99@outlook.com>	gary chen <gary_chen@mail.com>;	网站价钱
wang eric <eric_wang99@outlook.com>	gary chen <gary_chen@mail.com>;	连结
wang eric <eric_wang99@outlook.com>	gary chen <gary_chen@mail.com>;	连结
wang eric <eric_wang99@outlook.com>	gary chen <gary_chen@mail.com>;	Re: 确认买买买
wang eric <eric_wang99@outlook.com>	gary chen <gary_chen@mail.com>;	发票

The email content is as follows:

发件人: wang eric <eric\_wang99@outlook.com>  
 收件人: gary chen <gary\_chen@mail.com>;  
 邮件主题: 网站价钱  
 内容: Gary

iCloud 网站源代码的价钱要一千块钱。  
 关于枪或刀就有一点难说, 这样吧, 我给你一些连结, 你去看看吧

Eric  
 发送时间: 2017-10-19 20:21:18  
 服务器接收时间: 2017-10-19 20:21:22  
 附件个数: 1  
 邮件中转IP: 10.152.250.51; 10.152.250.54; 10.152.251.13; 10.152.251.156; 15.20.77.10; 40.92.254.73; 74.208.5.22  
 删除状态: 正常

CSDN @A349 奇乃正

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

```

文件名: icloud2.png
文件扩展名: png
逻辑大小(字节): 54,090
访问时间: 2017-10-20 16:02:26
创建时间: 2017-10-18 19:40:47
修改时间: 2017-10-18 19:40:47
文件类型: PNG图片
文件分类: 图片
描述: 文件, 存档
物理大小(字节): 57,344
物理位置: 52,453,007,360
物理扇区: 102,447,280
MD5值: C9FBFAF3C45492C40FEB83A83217F146
SHA-1值: 514DDC4F5D78246773BD5595E3C855ADB58406D0
SHA-256值: A1DE704BC4DC0F4AB26736920BC64D9F33B2A61CC8D841A8EF77F9EF607082C2
原始路径: E:\案例镜像\NCFC(Personal).e01\分区3_本地磁盘[E]:\2017-10-18\icloud2.png
完整路径: 17个人\E:\案例镜像\NCFC(Personal).e01\分区3_本地磁盘[E]:\2017-10-18\icloud2.png

```

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

```

文件名: Screenshot 3.png
文件扩展名: png
逻辑大小(字节): 1,523,799
访问时间: 2017-10-27 18:44:46
创建时间: 2017-10-27 18:44:45
修改时间: 2017-10-27 18:44:46
文件类型: PNG图片
文件分类: 图片
描述: 文件, 存档
物理大小(字节): 1,527,808
物理位置: 55,587,737,600
物理扇区: 108,569,800
MD5值: 4C57A45B8DA5EA01E5EB7D875F94A7B8
SHA-1值: DFOA2A2E96456BFEB3FA490C22FEF935E35A8B12
SHA-256值: 939A7C96F88C40DA120FA03BE2F63A8B48ABEDB266F588FBA6B5063DEBEF6EA7
原始路径: E:\案例镜像\NCFC(Personal).e01\分区3_本地磁盘[E]:\2017-10-27\Screenshot 3.png
完整路径: 17个人\E:\案例镜像\NCFC(Personal).e01\分区3_本地磁盘[E]:\2017-10-27\Screenshot 3.png

```

	<b>33</b>	<b>Gary的计算机系统时区是什么??</b>
√	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

```

文件名: icloud2.png
文件扩展名: png
逻辑大小(字节): 54,090
访问时间: 2017-10-20 16:02:26
创建时间: 2017-10-18 19:40:47
修改时间: 2017-10-18 19:40:47
文件类型: PNG 图片
文件分类: 图片
签名: 匹配
描述: 文件, 存档
物理大小(字节): 57,344
物理位置: 52,463,007,360
物理扇区: 102,447,280
MD5值: C98FFAF3C45492C40F8B83A63217F140
SHA-1值: 514DC4F5D78246773BD55996EC855ADE58406D0
SHA-256值: A1DE704BC4DC0F44B26736920BC64D9F33E2A61CC8D841A88F77F9EF607082C2
原始路径: E:\镜像\2017美亚杯取证大赛\2017个人赛\案例镜像\WCFC(Personal).e01\分区3_本地磁盘[E]:\2017-10-18\icloud2.png
完整路径: 2017年美亚杯个人赛[E:\镜像\2017美亚杯取证大赛\2017个人赛\案例镜像\WCFC(Personal).e01\分区3_本地磁盘[E]:\2017-10-18\icloud2.png

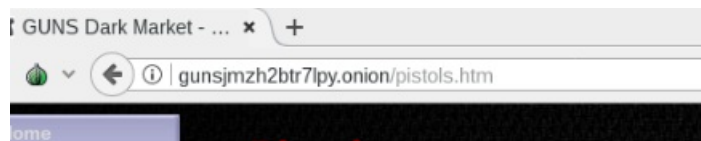
```



CSDN @A349 奇乃正

	<b>34</b>	<b>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？</b>
	A.	<a href="http://gunsdtk58tolcre.onion">http://gunsdtk58tolcre.onion</a>
√	B.	<a href="http://gunsjmzh2btr7lpy.onion">http://gunsjmzh2btr7lpy.onion</a>
	C.	<a href="http://thegunstorelasvegas.com">thegunstorelasvegas.com</a>
	D.	<a href="http://cabelas.com">cabelas.com</a>
	E.	<a href="http://hyattgunstore.com">hyattgunstore.com</a>

解析：找到相应图片，找到网址即可



	<b>35</b>	<b>Gary的笔记本电脑曾经下载过多少张有关恐怖组织的图片？</b>
	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

	<b>36</b>	<b>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>
	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

```

Gary

给你一个云盘，自己去看看
http://mantech.mo0o.com:8000
登录名：duncan@mo0o.com
密码：qazwsxedc

Eric

On 2017/10/30 12:12, gary chen wrote:
> Eric,
>
> 我真的想买，你有没有结构图？
>
> Gary
>

```

CSDN @A349 奇乃正

	37	下列哪项是上述私有云盘的网址？
	A.	http://mantech.mo0o.cn
√	B.	<a href="http://mantech.mo0o.com">http://mantech.mo0o.com</a>
	C.	http://mo0o.com
	D.	http://mantech.com
	E.	http://23.54.45.113

解析：查找相关邮件

Gary

给你一个云盘，自己去看看

<http://mantech.mooo.com:8000>

登录名：duncan@mooo.com

密码：qazwsxedc

Eric

On 2017/10/30 12:12, gary chen wrote:

> Eric,

>

> 我真的想买，你有没有结构图？

>

> Gary

>

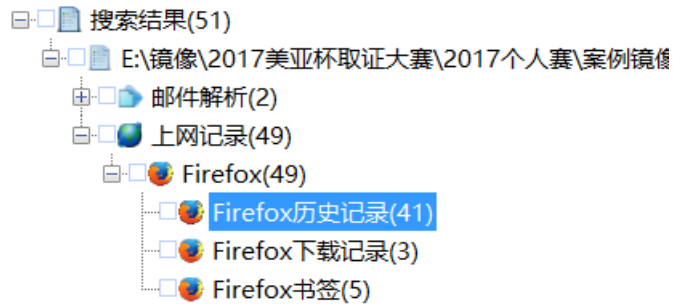
CSDN @A349 奇乃正

	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



< CSDN @A349 奇乃正 >

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

导出	加入摘要	跳转到源文件	打开关联文件
序号	URL地址	标题	最近访问时间
<input type="checkbox"/> 1	<a href="http://mantech.mooc.com:8000/">http://mantech.mooc.com:8000/</a>	Private Seafile	2017-10-30 12:42:11
<input type="checkbox"/> 2	<a href="http://mantech.mooc.com:8000/">http://mantech.mooc.com:8000/</a>	Private Seafile	2017-10-30 15:08:45
<input type="checkbox"/> 3	<a href="http://mantech.mooc.com:8000/">http://mantech.mooc.com:8000/</a>	Private Seafile	2017-10-30 15:11:44
<input type="checkbox"/> 4	<a href="http://mantech.mooc.com:8000/accounts/login?next=/">http://mantech.mooc.com:8000/accounts/login?next=/</a>		2017-10-30 12:42:11
<input type="checkbox"/> 5	<a href="http://mantech.mooc.com:8000/accounts/login?next=/">http://mantech.mooc.com:8000/accounts/login?next=/</a>		2017-10-30 15:08:45
<input type="checkbox"/> 6	<a href="http://mantech.mooc.com:8000/accounts/login/?next=/">http://mantech.mooc.com:8000/accounts/login/?next=/</a>	登录 - Private Seafile	2017-10-30 12:42:11

41	在上述加密磁区内，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	
<input checked="" type="checkbox"/> 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



序号	文件名称	保存路径	资源URL	临时路径	下载开始时间	下载结束时间	下载页面	已下载
1	IMG_20171027_222426_9433.GIF	E:/2017-10-30/M...	http://mantech.mooc.com:8000/repo/...		2017-10-30 15:14...	2017-10-30 15:14...		1,203,4...

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。

文件名称: invoice.zip  
 文件扩展名: zip  
 逻辑大小(字节): 3,223,545  
 访问时间: 2017-10-31 12:18:58  
**创建时间: 2017-10-31 12:18:54**  
 修改时间: 2017-10-31 12:18:58  
 文件类型: Zip压缩文件  
 文件分类: 压缩文件  
 签名: 匹配  
 描述: 文件, 存档  
 物理大小(字节): 3,223,552  
 物理位置: 22,335,209,472  
 物理扇区: 43,623,456  
 原始路径: E:\2017个人赛\案例镜像\NCFE(Personal).e01\分区2\_本地磁盘[D]:\Users\Gary\Downloads\invoice.zip  
 完整路径: 2017个人\E:\2017个人赛\案例镜像\NCFE(Personal).e01\分区2\_本地磁盘[D]:\Users\Gary\Downloads\invoice.zip

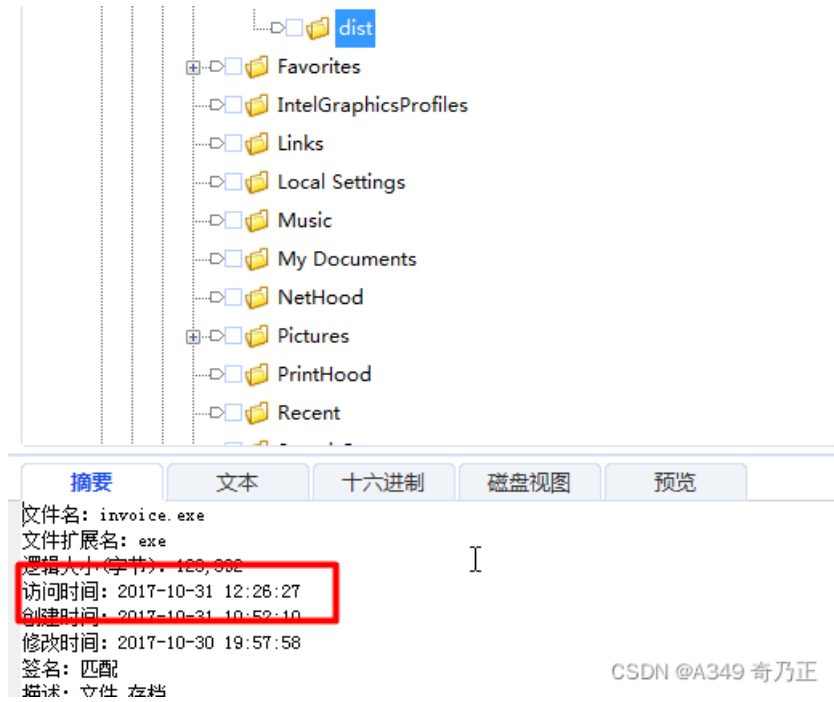
序号	文件名称	创建时间	访问时间	最后修改时间	删除时间	文件大小(字节)
1	invoice.zip	2017-10-31 12:18:54	2017-10-31 12:18...	2017-10-31 12:18...		3,223,545
2	invoice.zip-Zone.Identifier		2017-10-31 12:18:54			26

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？
----	--

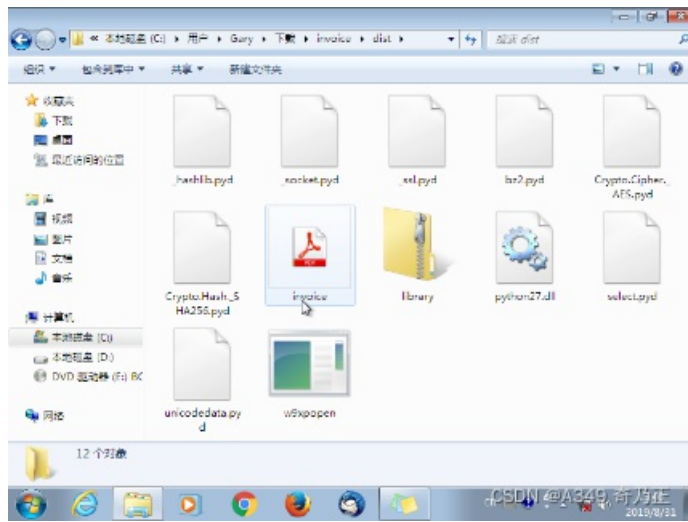
D.	2017-10-31 10:52:10
E.	2017-10-31 12:18:54

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

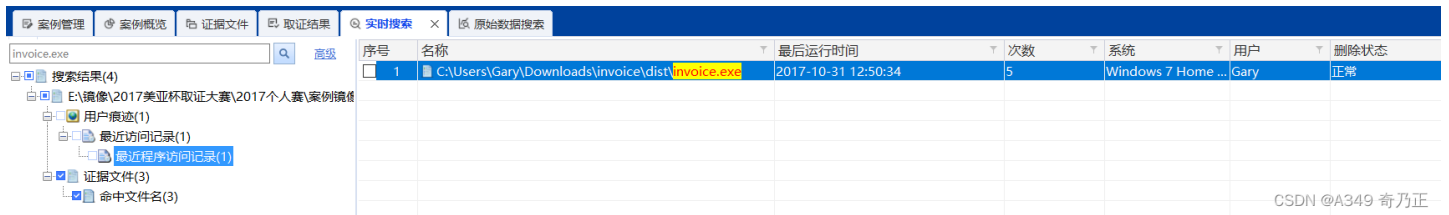
序号	文件名	标签	文件扩展名	逻辑大小(字节)	访问时间	创建时间	修改时间	删除时间	文件类型
1	hashlib.pyd		pyd	1,016,832	2017-10-31 12:29:55	2017-10-30 19:57:50	2016-12-17 20:46:14		
2	socket.pyd		pyd	46,592	2017-10-30 19:57:50	2017-10-30 19:57:50	2016-12-17 20:45:20		
3	ssl.pyd		pyd	1,410,048	2017-10-30 19:57:50	2017-10-30 19:57:50	2016-12-17 20:45:56		
4	bz2.pyd		pyd	71,168	2017-10-30 19:57:50	2017-10-30 19:57:50	2016-12-17 20:44:38		
5	Crypto.Cipher_AES.pyd		pyd	29,184	2017-10-31 12:29:55	2017-10-30 19:57:50	2012-09-28 04:28:48		
6	Crypto.Hash_SHA256.pyd		pyd	10,240	2017-10-30 19:57:50	2017-10-30 19:57:50	2012-09-28 04:28:48		
7	invoice.exe		exe	123,392	2017-10-31 12:26:27	2017-10-31 10:52:10	2017-10-30 19:57:58		
8	library.zip		zip	1,720,699	2017-10-31 12:29:55	2017-10-30 19:57:50	2017-10-30 18:24:35		Zip压缩文
9	_future_.pyc		pyc	4,103	2017-09-13 16:44:38	2017-09-13 16:44:38	2017-09-13 16:44:38		
10	_abcoll.pyc		pyc	23,604	2017-09-13 16:44:38	2017-09-13 16:44:38	2017-09-13 16:44:38		
11	hashlib.pyc		pyc	549	2017-10-30 18:24:34	2017-10-30 18:24:34	2017-10-30 18:24:34		
12	socket.pyc		pyc	546	2017-10-30 18:24:34	2017-10-30 18:24:34	2017-10-30 18:24:34		
13	ssl.pyc		pyc	537	2017-10-30 18:24:34	2017-10-30 18:24:34	2017-10-30 18:24:34		

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



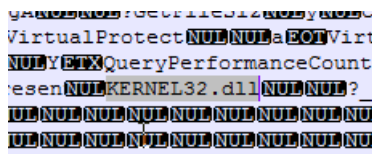
48	上述\User\Gary\Downloads\invoice\dist\invoice.exe文件是由什么程序编写？	
A.		LISP
B.		C++
C.		Visual Basic
√ D.		Python
E.		Java

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\invoice.exe
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\kernel132.dll
invoice.exe	3020	Load Image	C:\Windows\SysWOW64\kernel132.dll
invoice.exe	3020	Load Image	C:\Windows\System32\user32.dll
invoice.exe	3020	Load Image	C:\Windows\SysWOW64\kernel132.dll
invoice.exe	3020	Load Image	C:\Windows\SysWOW64\KernelBase.dll
invoice.exe	3020	Load Image	C:\Windows\winsxs\x86_microsoft.vc90.c...
invoice.exe	3020	Load Image	C:\Users\DNG\Desktop\invoice\dist\python...
invoice.exe	3020	Load Image	C:\Windows\SysWOW64\user32.dll
invoice.exe	3020	Load Image	C:\Windows\SysWOW64\kernel132.dll
invoice.exe	3020	Load Image	C:\Windows\SysWOW64\ipk.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

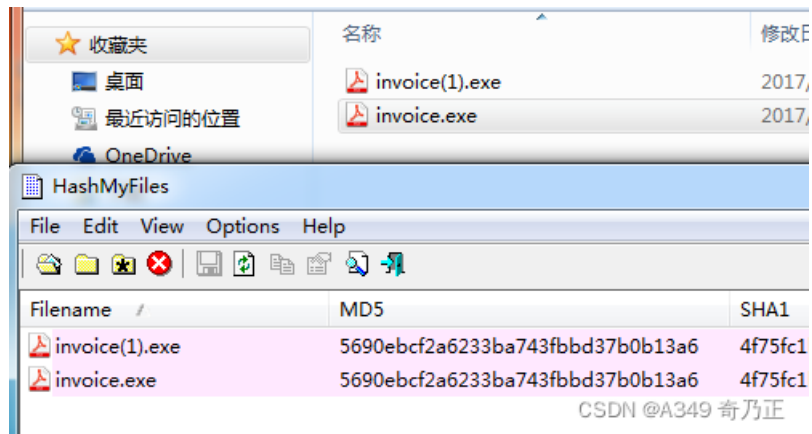
解析：

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.	前者是后者的副本
√ B.	后者是前者的副本
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	根据勒索信息的显示，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	根据勒索信息的显示，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：

# 文件将永远丢失

## 24日 15时 58分钟 36秒

要获取您的文件，请发送1比特币（\$10,000）到以下比特币钱包：**1KcjhpknwGWh5QYgPx5hYGuzbZpewgBszh**

帮助购买比特币

CSDN @A349 奇乃正

54	根据勒索訊息的显示，下列哪个是与勒索案件有关的比特币钱包？	
	A.	1KcjhpknwGWh5QYgPx5hYGuzbZpewgBszh
√	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：

逻辑大小(字节): 60,777  
访问时间: 2017-10-31 12:52:14  
创建时间: 2017-10-31 12:52:14  
修改时间: 2017-10-31 12:52:14  
文件类型: PNG图片  
文件分类: 图片  
签名: 匹配  
描述: 文件, 存档  
物理大小(字节): 61,440  
物理位置: 16,902,537,216  
物理扇区: 33,012,768  
原始路径: E:\案例镜像\NCFC(Personal).e01\分区2\_本地磁盘[D]:\Users\Gary\Desktop\screen.png  
完整路径: 17个人\E:\案例镜像\NCFC(Personal).e01\分区2\_本地磁盘[D]:\Users\Gary\Desktop\screen.png

CSDN @A349 奇乃正

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

```

文件名: mk
逻辑大小(字节): 64
访问时间: 2017-10-26 17:36:22
创建时间: 2017-10-19 15:59:16
修改时间: 2017-10-19 15:59:16
签名: 未知
描述: 文件, 存档, 隐藏
物理大小(字节): 64
物理位置: 3,375,395,088
物理扇区: 6,592,568
原始路径: E:\案例镜像\NCFC(Personal).e01\分区2_本地磁盘[D]:\mk
完整路径: 17个人\E:\案例镜像\NCFC(Personal).e01\分区2_本地磁盘[D]:\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