2018第四届美亚杯中国电子数据取证大赛个人赛write up

原创

奇乃正 于 2022-01-04 09:27:23 发布 3078 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/122296056

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

“美亚杯”第四届中国电子数据取证竞赛-资格赛

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！

本次比赛共1 个章节, 50 个小题, 比赛时长118 分钟, 总共100分

单项选择

1. Victor的笔记本电脑已成功取证并制作成法证映像档 (Forensic Image)，下列哪个是其MD5哈希值? (2分)

A. FC20782C21751AB76B2A93F3A17922D0

B. 882114D62E713DEA34C270CF2F1C69D2

C. A0BB016160CFB3A0BB0161661670CFB3

D. 917ED59083C8B35C54D3FCBFE4C4BB0B

E. FC20782C21751BA76B2A93F3A17922D0

解析：取证大师直接分析得出

2. 根据法证映像档 (Forensic Image)，确定原笔记本内有多少个硬盘分区? (2分)

A. 1

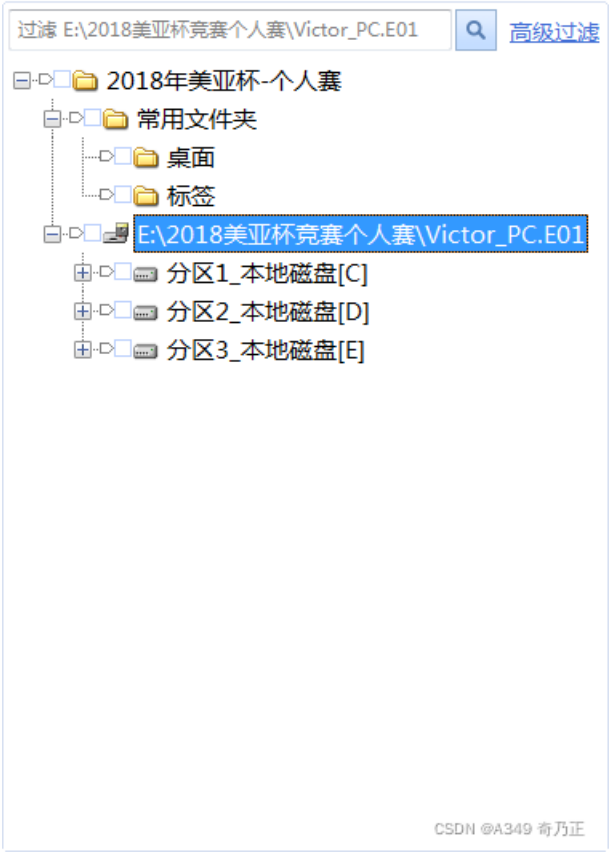
B. 2

C. 3

D. 4

E. 5

解析：取证大师直接分析得出



3. 你能找到硬盘操作系统分区内的开始逻辑区块地址（LBA）? (答案格式: 扇区, Sector) (2分)

A. 0

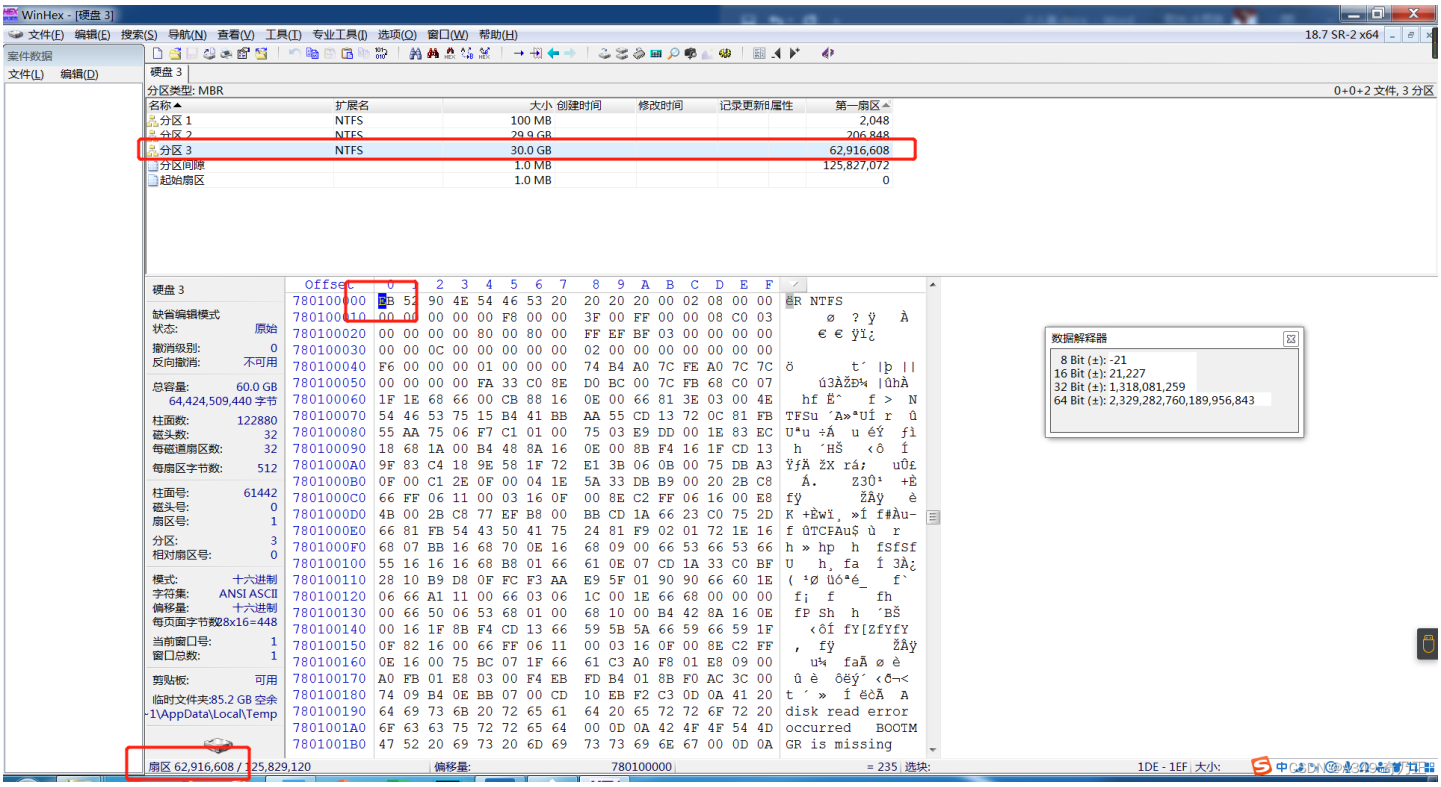
B. 2408

C. 1048576

D. 62916608

E. 32213303296

解析：winhex直接查看



4. 你能找到硬盘操作系统分区的物理大小吗 (字节byte)? (2分)

A. 62709760

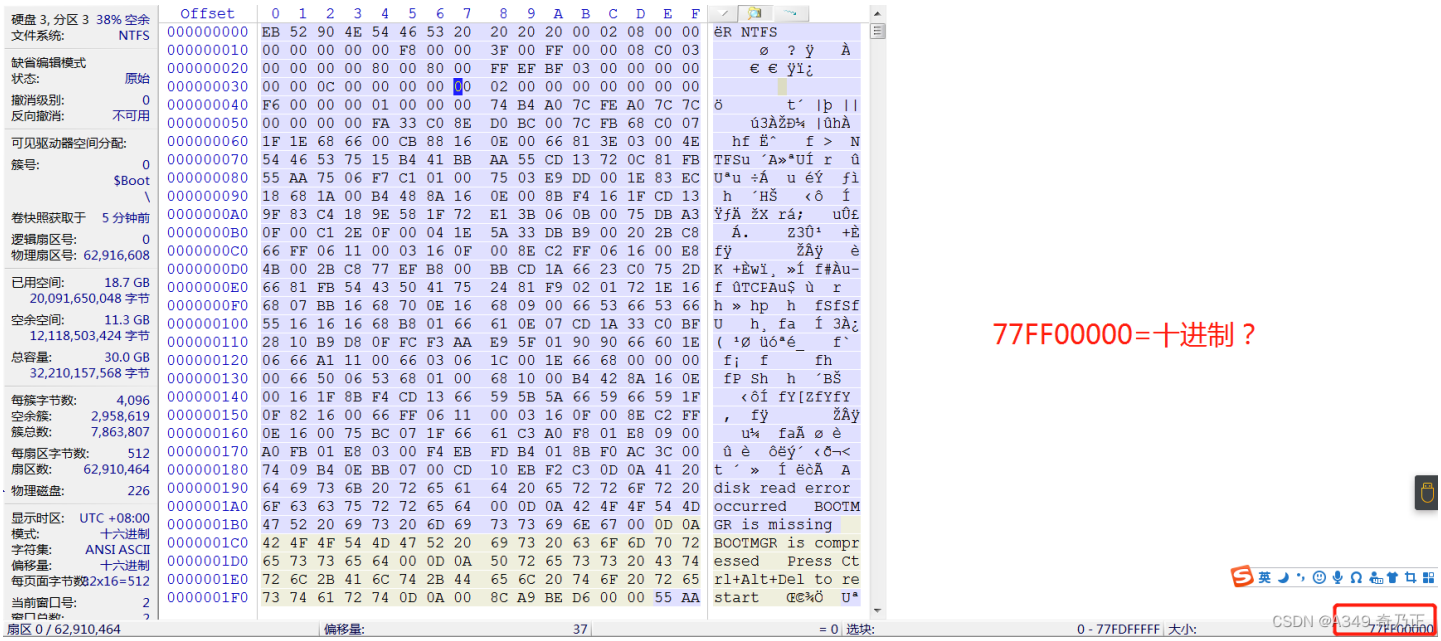
B. 62910464

C. 104857600

D. 32107397120

E. 32210157568

解析：winhex直接查看



5. 操作系统分区的文件系统是哪种? (2分)

A. FAT32

B. EXFAT

C. NTFS

D. EXT3

E. HFS+

解析：取证大师直接分析得出

6. 操作系统分区，每个簇(Cluster)包含几个扇区(sectors)? (2分)

A. 2

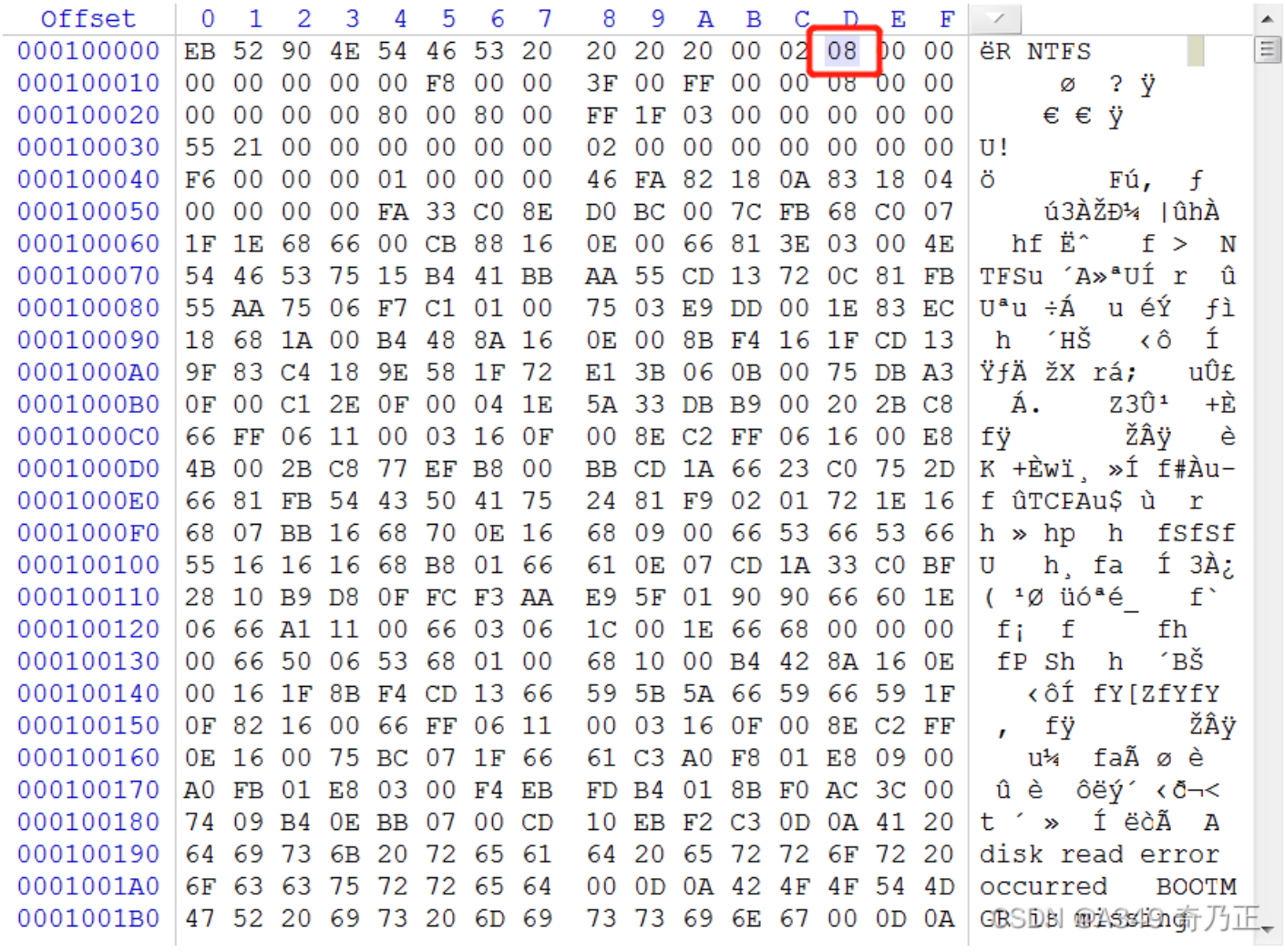
B. 4

C. 6

D. 8

E. 16

解析：winhex直接查看



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000100000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	ëR NTFS
000100010	00	00	00	00	00	F8	00	00	3F	00	FF	00	00	08	00	00	ø ? ÿ
000100020	00	00	00	00	80	00	80	00	FF	1F	03	00	00	00	00	00	€ € ÿ
000100030	55	21	00	00	00	00	00	00	02	00	00	00	00	00	00	00	U!
000100040	F6	00	00	00	01	00	00	00	46	FA	82	18	0A	83	18	04	ö Fú, ƒ
000100050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07	ú3ÀŽĐ¼ |ûhÀ
000100060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	hf Ë^ f > N
000100070	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB	TFSu ´A»ªUÍ r û
000100080	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	Uªu ÷Á u éÝ ƒì
000100090	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	h ´HŠ ‹ô Í
0001000A0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3	ŸƒÄ žX rá; uÛ£
0001000B0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	Á. Z3Û¹ +È
0001000C0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fÿ ŽÂÿ è
0001000D0	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D	K +Èwï¸ »Í f#Àu-
0001000E0	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16	f ûTCPAu$ ù r
0001000F0	68	07	BB	16	68	70	0E	16	68	09	00	66	53	66	53	66	h » hp h fSfSf
000100100	55	16	16	16	68	B8	01	66	61	0E	07	CD	1A	33	C0	BF	U h¸ fa Í 3À¿
000100110	28	10	B9	D8	0F	FC	F3	AA	E9	5F	01	90	90	66	60	1E	(¹Ø üóªé_ f`
000100120	06	66	A1	11	00	66	03	06	1C	00	1E	66	68	00	00	00	f¡ f fh
000100130	00	66	50	06	53	68	01	00	68	10	00	B4	42	8A	16	0E	fP Sh h ´BŠ
000100140	00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F	‹ôÍ fY[ZfYfY
000100150	0F	82	16	00	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	, fÿ ŽÂÿ
000100160	0E	16	00	75	BC	07	1F	66	61	C3	A0	F8	01	E8	09	00	u¼ faÃ ø è
000100170	A0	FB	01	E8	03	00	F4	EB	FD	B4	01	8B	F0	AC	3C	00	û è ôëý´ ‹ð¬<
000100180	74	09	B4	0E	BB	07	00	CD	10	EB	F2	C3	0D	0A	41	20	t ´ » Í ëòÃ A
000100190	64	69	73	6B	20	72	65	61	64	20	65	72	72	6F	72	20	disk read error
0001001A0	6F	63	63	75	72	72	65	64	00	0D	0A	42	4F	4F	54	4D	occurred BOOTM
0001001B0	47	52	20	69	73	20	6D	69	73	73	69	6E	67	00	0D	0A	GR is missing

7. 在操作系统分区内，$MFT的物理起始扇区位置(Starting physical sector)是什么？
(2分)

A. 62,919,936

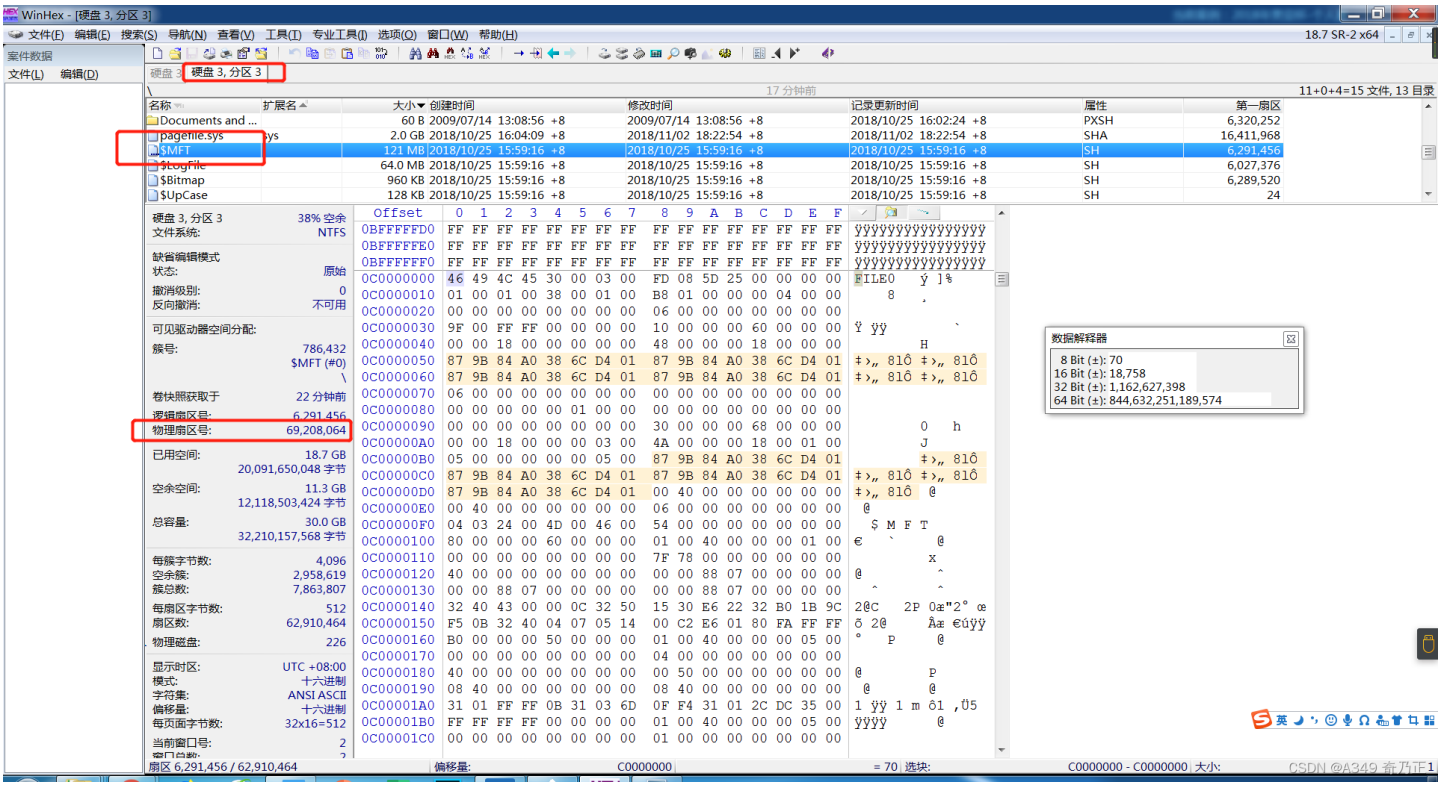
B. 67,086,648

C. 68,942,784

D. 69,208,064

E. 79,865,960

解析：winhex直接查看



8. 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）(2分)

A. 2018-10-25 08:08 UTC

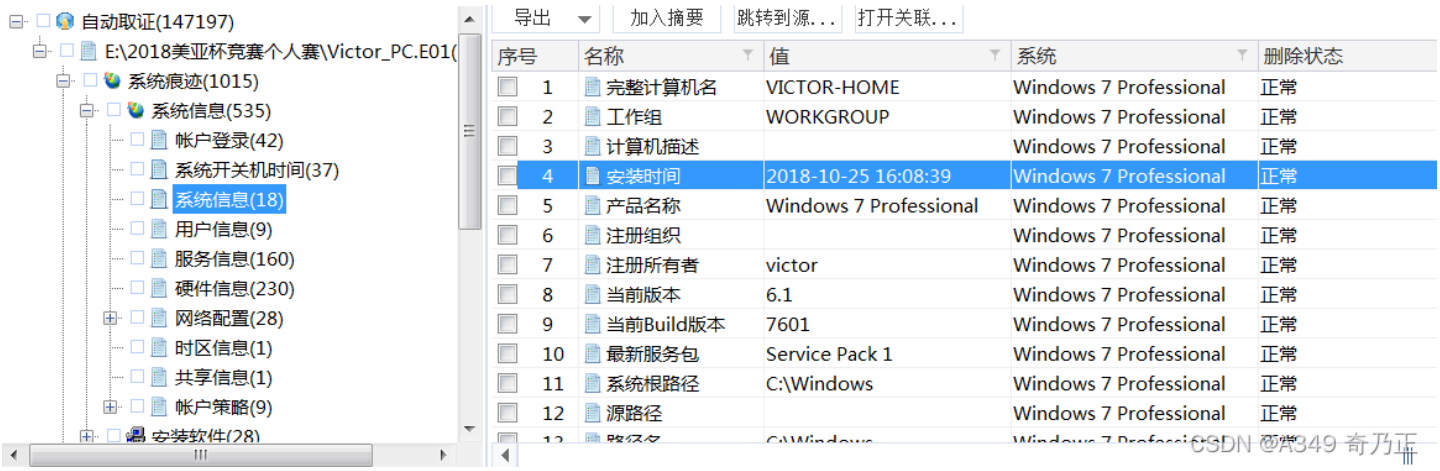
B. 2018-10-25 08:09 UTC

C. 2018-10-25 08:10 UTC

D. 2018-10-25 08:11 UTC

E. 2018-10-25 08:12 UTC

解析：取证大师直接分析得出



9. 用户“victor " 的唯一标识符(SID)是什么？（答案格式：RID） (2分)

A. 1001

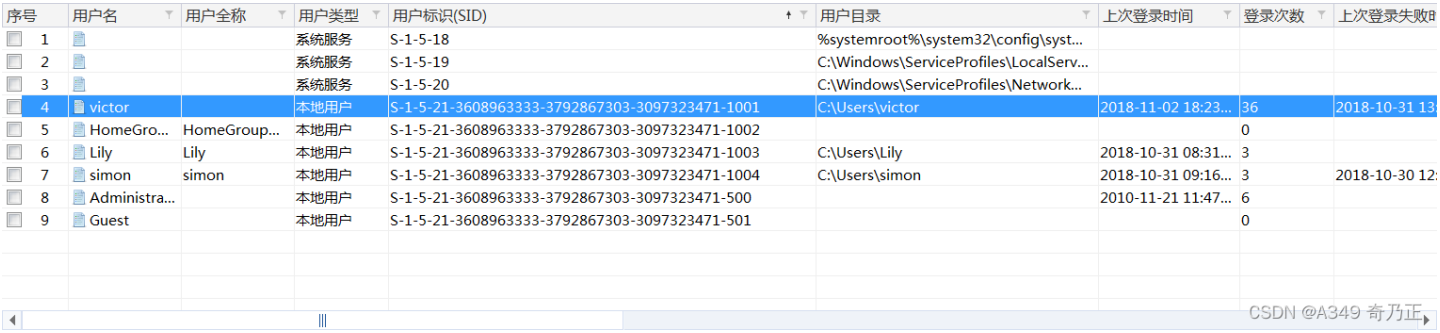
B. 1002

C. 1003

D. 1004

E. 1005

解析：取证大师直接分析得出



10. 用户“Lily " 的唯一标识符(SID)是什么？（答案格式：RID） (2分)

A. 1001

B. 1002

C. 1003

D. 1004

E. 1005

解析：取证大师直接分析得出

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	上次登录失败时
1			系统服务	S-1-5-18	%systemroot%\system32\config\syst...			
2			系统服务	S-1-5-19	C:\Windows\ServiceProfiles\LocalServ...			
3			系统服务	S-1-5-20	C:\Windows\ServiceProfiles\Network...			
4	victor		本地用户	S-1-5-21-3608963333-3792867303-3097323471-1001	C:\Users\victor	2018-11-02 18:23...	36	2018-10-31 13:
5	HomeGro...	HomeGroup...	本地用户	S-1-5-21-3608963333-3792867303-3097323471-1002			0	
6	Lily	Lily	本地用户	S-1-5-21-3608963333-3792867303-3097323471-1003	C:\Users\Lily	2018-10-31 08:31...	3	
7	simon	simon	本地用户	S-1-5-21-3608963333-3792867303-3097323471-1004	C:\Users\simon	2018-10-31 09:16...	3	2018-10-30 12:
8	Administra...		本地用户	S-1-5-21-3608963333-3792867303-3097323471-500		2010-11-21 11:47...	6	
9	Guest		本地用户	S-1-5-21-3608963333-3792867303-3097323471-501			0	

11. Victor上一次更改系统登入密码是？（答案格式 一“本地时间 "：YYYY-MM-DD HH:MM +8） (2分)

A. 2018-11-01 16:08 +8

B. 2018-11:01 14:15 +8

C. 2018-10-26 17:00 +8

D. 2018-10-25 08:08 +8

E. 2018-10-25 16:08 +8

解析：取证大师直接分析得出

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	上次密码设置时间	登录次数	上次登录失
1	Administra...		本地用户	S-1-5-21-3608963333-3792867303-3...		2010-11-21 11:47:20	2010-11-21 11:57:24	6	
2	Guest		本地用户	S-1-5-21-3608963333-3792867303-3...				0	
3	victor		本地用户	S-1-5-21-3608963333-3792867303-30...	C:\Users\victor	2018-11-02 18:23:03	2018-10-25 16:08:37	36	2018-10-31
4	HomeGro...	HomeGroup...	本地用户	S-1-5-21-3608963333-3792867303-30...			2018-10-25 1	2018-10-25 16:08:37	
5	Lily	Lily	本地用户	S-1-5-21-3608963333-3792867303-30...	C:\Users\Lily	2018-10-31 08:31:09	2018-10-30 12:30:40	3	
6	simon	simon	本地用户	S-1-5-21-3608963333-3792867303-30...	C:\Users\simon	2018-10-31 09:16:01	2018-10-30 12:30:27	3	2018-10-3
7			系统服务	S-1-5-18	%systemroot%\system32\config\syst...				
8			系统服务	S-1-5-19	C:\Windows\ServiceProfiles\LocalServ...				
9			系统服务	S-1-5-20	C:\Windows\ServiceProfiles\Network...				

12. Lily上一次更改系统登入密码是？（答案格式 一“本地时间 "：YYYY-MM-DD HH:MM +8） (2分)

A. 2018-11-01 03:02:01 +8

B. 2018-11:02 11:13:33 +8

C. 2018-10-26 17:00:45 +8

D. 2018-10-30 12:30:40 +8

E. 2018-10-27 12:08:37 +8

解析：取证大师直接分析得出

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	上次密码设置时间	登录次数	上次登录失
1	Administra...		本地用户	S-1-5-21-3608963333-3792867303-3...		2010-11-21 11:47:20	2010-11-21 11:57:24	6	
2	Guest		本地用户	S-1-5-21-3608963333-3792867303-3...				0	
3	victor		本地用户	S-1-5-21-3608963333-3792867303-30...	C:\Users\victor	2018-11-02 18:23:03	2018-10-25 16:08:37	36	2018-10-31
4	HomeGro...	HomeGroup...	本地用户	S-1-5-21-3608963333-3792867303-30...			2018-10-25 16:08:37	0	
5	Lily	Lily	本地用户	S-1-5-21-3608963333-3792867303-30...	C:\Users\Lily	2018-10-31 08:31:09	2018-10-30 12:30:40	3	
6	simon	simon	本地用户	S-1-5-21-3608963333-3792867303-30...	C:\Users\simon	2018-10-31 09:16:01	2018-10-30 12:30:27	3	2018-10-3
7			系统服务	S-1-5-18	%systemroot%\syste	C:\Users\simon			
8			系统服务	S-1-5-19	C:\Windows\ServiceProfiles\LocalServ...				
9			系统服务	S-1-5-20	C:\Windows\ServiceProfiles\Network...				

13. Victor 总共登录系统多少次? (2分)

A. 3

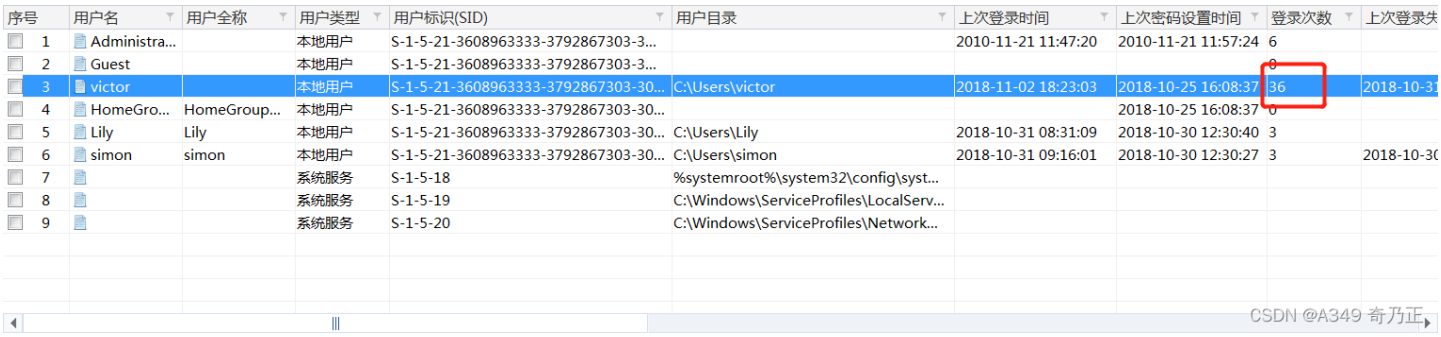
B. 16

C. 33

D. 36

E. 45

解析：取证大师直接分析得出



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	上次密码设置时间	登录次数	上次登录失
1	Administra...		本地用户	S-1-5-21-3608963333-3792867303-3...		2010-11-21 11:47:20	2010-11-21 11:57:24	6	
2	Guest		本地用户	S-1-5-21-3608963333-3792867303-3...				0	
3	victor		本地用户	S-1-5-21-3608963333-3792867303-30...	C:\Users\victor	2018-11-02 18:23:03	2018-10-25 16:08:37	36	2018-10-31
4	HomeGro...	HomeGroup...	本地用户	S-1-5-21-3608963333-3792867303-30...			2018-10-25 16:08:37	0	
5	Lily	Lily	本地用户	S-1-5-21-3608963333-3792867303-30...	C:\Users\Lily	2018-10-31 08:31:09	2018-10-30 12:30:40	3	
6	simon	simon	本地用户	S-1-5-21-3608963333-3792867303-30...	C:\Users\simon	2018-10-31 09:16:01	2018-10-30 12:30:27	3	2018-10-30
7			系统服务	S-1-5-18	%systemroot%\system32\config\syst...				
8			系统服务	S-1-5-19	C:\Windows\ServiceProfiles\LocalServ...				
9			系统服务	S-1-5-20	C:\Windows\ServiceProfiles\Network...				

14. 以下哪个帐号已经被禁用? (2分)

A. Administrator

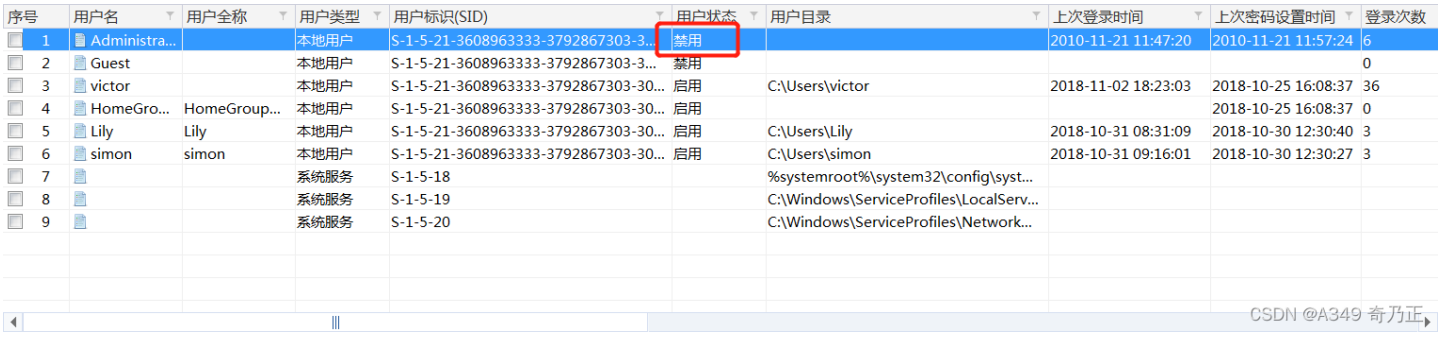
B. victor

C. Lily

D. simon

E. 以上皆不是

解析：取证大师直接分析得出



序号	用户名	用户全称	用户类型	用户标识(SID)	用户状态	用户目录	上次登录时间	上次密码设置时间	登录次数
1	Administra...		本地用户	S-1-5-21-3608963333-3792867303-3...	禁用		2010-11-21 11:47:20	2010-11-21 11:57:24	6
2	Guest		本地用户	S-1-5-21-3608963333-3792867303-3...	禁用				0
3	victor		本地用户	S-1-5-21-3608963333-3792867303-30...	启用	C:\Users\victor	2018-11-02 18:23:03	2018-10-25 16:08:37	36
4	HomeGro...	HomeGroup...	本地用户	S-1-5-21-3608963333-3792867303-30...	启用			2018-10-25 16:08:37	0
5	Lily	Lily	本地用户	S-1-5-21-3608963333-3792867303-30...	启用	C:\Users\Lily	2018-10-31 08:31:09	2018-10-30 12:30:40	3
6	simon	simon	本地用户	S-1-5-21-3608963333-3792867303-30...	启用	C:\Users\simon	2018-10-31 09:16:01	2018-10-30 12:30:27	3
7			系统服务	S-1-5-18		%systemroot%\system32\config\syst...			
8			系统服务	S-1-5-19		C:\Windows\ServiceProfiles\LocalServ...			
9			系统服务	S-1-5-20		C:\Windows\ServiceProfiles\Network...			

15. 以下哪个帐系统权限最低? (2分)

A. Administrator

B. victor

C. Lily

D. simon

E. 以上权限一样

解析：取证大师直接分析得出

序号	用户名	用户全称	用户类型	用户标识(SID)	用户状态	用户目录	所在用户组	上次登录时间	上次密码设置时
1	HomeGro...	HomeGroup...	本地用户	S-1-5-21-3608963333-3792867303-30...	启用				2018-10-25 16:0
2			系统服务	S-1-5-18		%systemroot%\system32\config\syst...			
3			系统服务	S-1-5-19		C:\Windows\ServiceProfiles\LocalServ...			
4			系统服务	S-1-5-20		C:\Windows\ServiceProfiles\Network...			
5	Administra...		本地用户	S-1-5-21-3608963333-3792867303-3...	禁用		Administrators	2010-11-21 11:47:20	2010-11-21 11:5
6	victor		本地用户	S-1-5-21-3608963333-3792867303-30...	启用	C:\Users\victor	Administrators	2018-11-02 18:23:03	2018-10-25 16:0
7	Lily	Lily	本地用户	S-1-5-21-3608963333-3792867303-30...	启用	C:\Users\Lily	Administrator...	2018-10-31 08:31:09	2018-10-30 12:3
8	Guest		本地用户	S-1-5-21-3608963333-3792867303-3...	禁用		Guests		
9	simon	simon	本地用户	S-1-5-21-3608963333-3792867303-30...	启用	C:\Users\simon	Users;Guests	2018-10-31 09:16:01	2018-10-30 12:3

16. 以下哪个帐号曾经远端登录系统? (2分)

A. Administrator

B. victor

C. Lily

D. simon

E. 远端登入已被禁止

解析：

17. 硬盘操作系统的版本? (2分)

A. Windows 7 Enterprise (32 位)

B. Windows 7 Enterprise (64 位)

C. Windows 7 Professional (32 位)

D. Windows 7 Professional (64 位)

E. Windows 7 Ultimate (64 位)

解析：取证大师直接分析得出

序号	名称	值	系统	删除状态
1	完整计算机名	VICTOR-HOME	Windows 7 Professional	正常
2	工作组	WORKGROUP	Windows 7 Professional	正常
3	计算机描述		Windows 7 Professional	正常
4	安装时间	2018-10-25 16:08:39	Windows 7 Professional	正常
5	产品名称	Windows 7 Professional	Windows 7 Professional	正常
6	注册组织		Windows 7 Professional	正常
7	注册所有者	victor	Windows 7 Professional	正常
8	当前版本	6.1	Windows 7 Professional	正常
9	当前Build版本	7601	Windows 7 Professional	正常
10	最新服务包	Service Pack 1	Windows 7 Professional	正常
11	系统根路径	C:\Windows	Windows 7 Professional	正常
12	源路径		Windows 7 Professional	正常
13	路径名	C:\Windows	Windows 7 Professional	正常
14	产品ID	00371-177-0000061-85...	Windows 7 Professional	正常
15	操作系统类型	64位	Windows 7 Professional	正常
16	最后一次正常关...	2018-11-02 18:47:51	Windows 7 Professional	正常
17	制造商		Windows 7 Professional	正常
18	型号		Windows 7 Professional	正常

18. 操作系统的最新服务包(Service Pack)版本号是什么? (2分)

A. Service Pack 1

B. Service Pack 2

C. Service Pack 3

D. Service Pack 4

E. Service Pack 5

解析：取证大师直接分析得出

序号	名称	值	系统	删除状态
1	完整计算机名	VICTOR-HOME	Windows 7 Professional	正常
2	工作组	WORKGROUP	Windows 7 Professional	正常
3	计算机描述		Windows 7 Professional	正常
4	安装时间	2018-10-25 16:08:39	Windows 7 Professional	正常
5	产品名称	Windows 7 Professional	Windows 7 Professional	正常
6	注册组织		Windows 7 Professional	正常
7	注册所有者	victor	Windows 7 Professional	正常
8	当前版本	6.1	Windows 7 Professional	正常
9	当前Build版本	7601	Windows 7 Professional	正常
10	最新服务包	Service Pack 1	Windows 7 Professional	正常
11	系统根路径	C:\Window	Windows 7 Professional	正常
12	源路径		Windows 7 Professional	正常
13	路径名	C:\Windows	Windows 7 Professional	正常
14	产品ID	00371-177-0000061-85...	Windows 7 Professional	正常
15	操作系统类型	64位	Windows 7 Professional	正常
16	最后一次正常关...	2018-11-02 18:47:51	Windows 7 Professional	正常
17	制造商		Windows 7 Professional	正常
18	型号		Windows 7 Professional	正常

Service Pack 1

19. 下列哪个是victor的默认打印机? (2分)

A. HP OfficeJet 250 Mobile Series

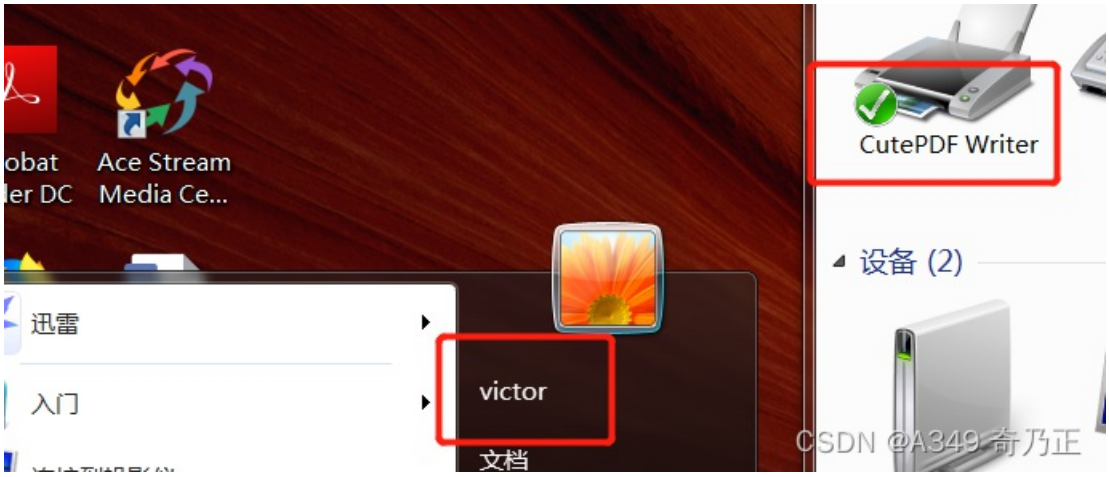
B. CutePDF Writer

C. Microsoft XPS Document Writer

D. PDF Complete

E. AL-M2330

解析：仿真系统中，在Victor用户下的控制面板中找到默认打印机



20. 在2018-10-31 08:29:32 +8时间, 账号simon曾经使用以下哪个文件? (2分)

A. Microsoft 商店.url

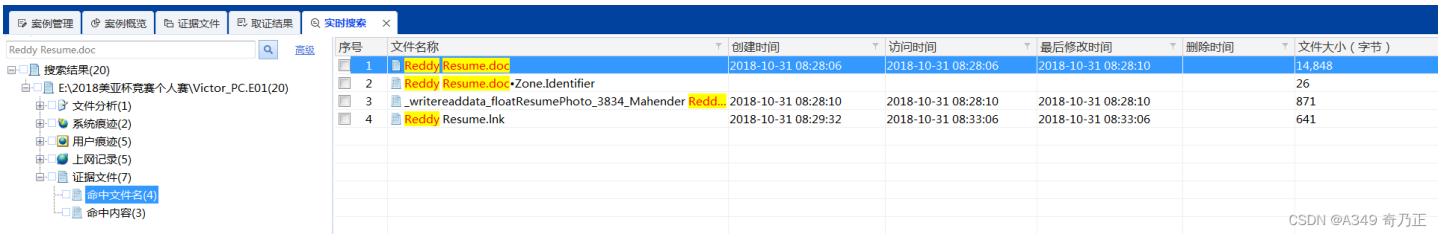
B. ug.jpeg

C. Reddy Resume.doc

D. grocerylistsDOTorg_Spreadsheet_v1_1.xls

E. InvoiceTemplate.docx

解析：对选项进行实时搜索得出。



21. 接上题，开启上述文件的程序是? (2分)

A. Internet Explorer

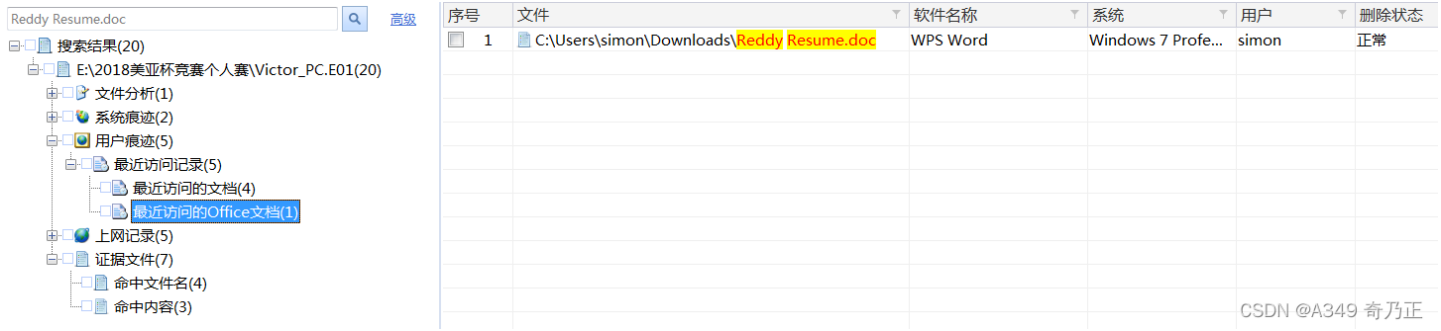
B. Firefox

C. 画图

D. WPS 表格

E. WPS 文字

解析：接上题图，取证大师直接分析得出



22. 以下哪个是victor的默认网页浏览器? (2分)

A. Internet Explorer

B. Google Chrome

C. 360浏览器

D. Firefox

E. 迅雷浏览器

解析：仿真系统Victor用户下，新建.html文件，可知默认浏览器。

23. victor的回收站里面有一张地图，以下哪个是这张地图原来的文件名? (2分)

A. 捕获.PNG

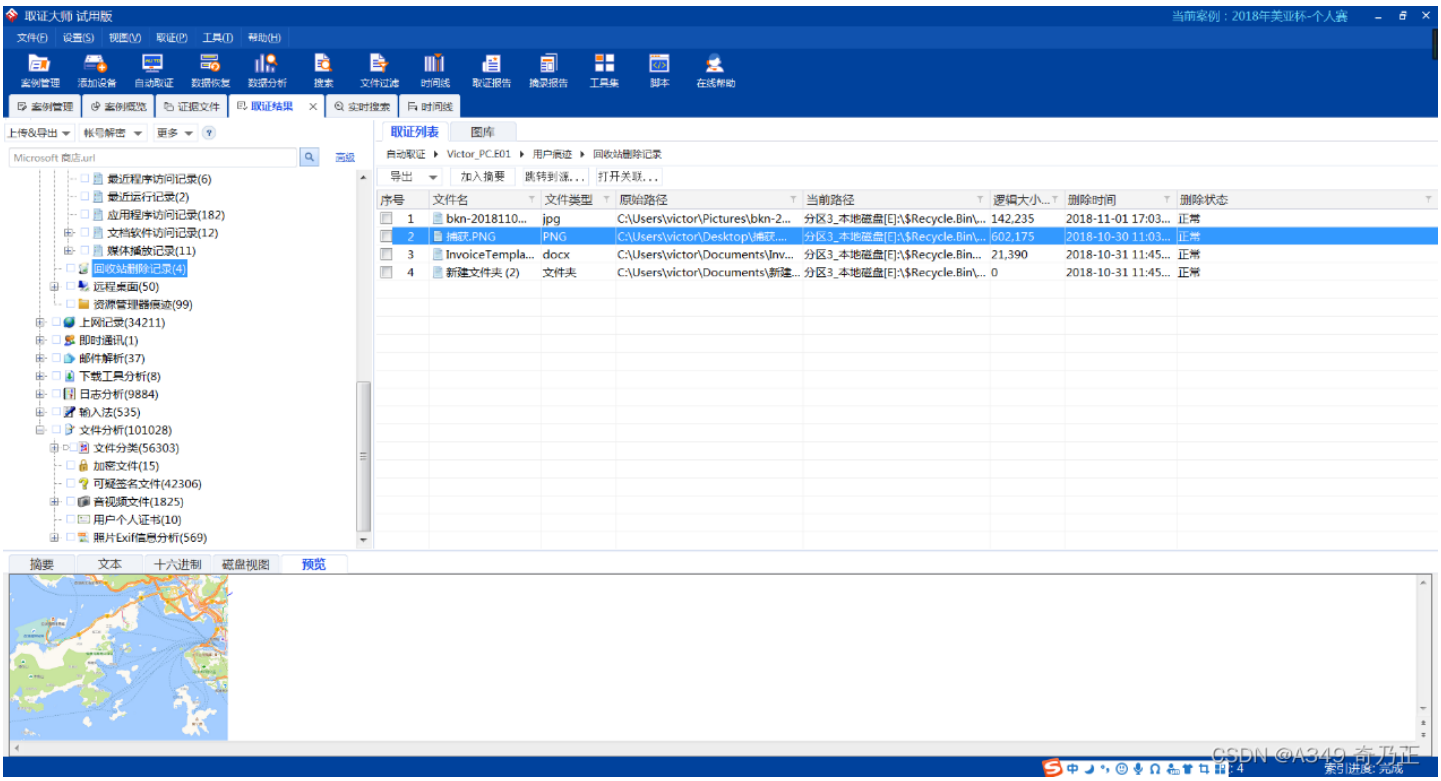
B. 抓取.PNG

C. Screenshot.PNG

D. Map.bmp

E. Map.jpg

解析：取证大师直接分析得出



24. 接上题，上述地图原来的储存路径是? (2分)

A. C:\Users\victor\Pictures

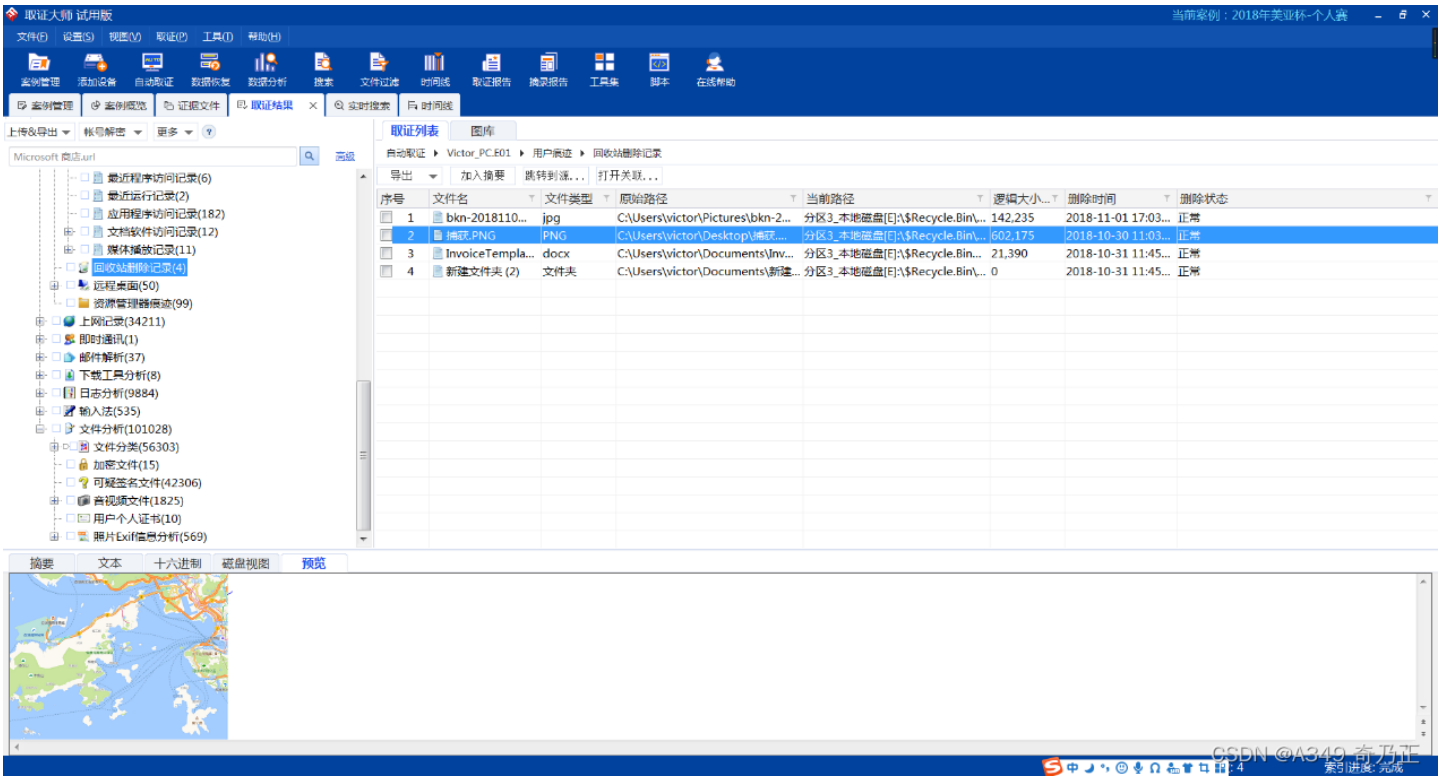
B. C:\Users\victor\Documents

C. C:\Users\victor\Desktop

D. C:\Users\victor\Downloads

E. C:\

解析：取证大师直接分析得出



25. 找出一个名为"request for quotation.lnk"的档案，并指出该LNK文件的目标路径?
(2分)

A. C:\Users\victor\Pictures

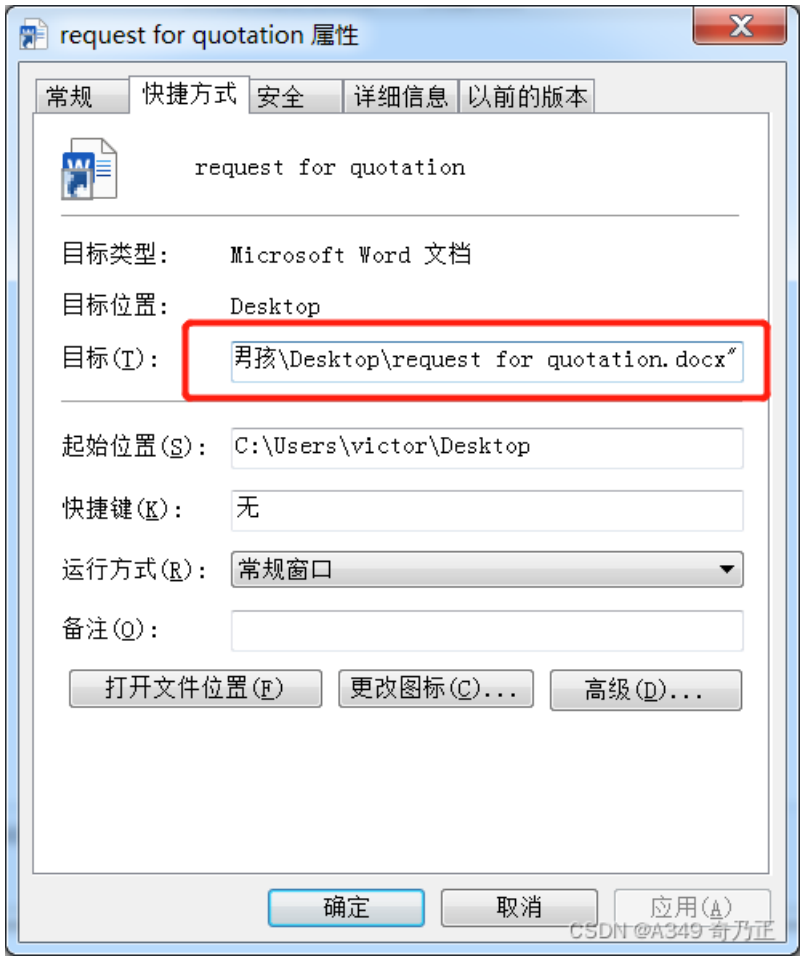
B. C:\Users\victor\Documents

C. C:\Users\victor\Desktop

D. C:\Users\victor\Downloads

E. C:\

解析：“C:\……\Desktop\request for quotation.docx”



26. 接上题，上述文件上一次开启的时间是？（答案格式 一“本地时间 " ：YYYY-MM-DD HH:MM:SS +8） (2分)

A. 2018-10-29 15:11:43 +8

B. 2018-10-29 19:24:16 +8

C. 2018-10-29 15:11:42 +8

D. 2018-11-01 14:51:25 +8

E. 2018-10-29 07:11:42 +8

解析：取证大师直接分析得出

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
10	CustomDestinations			4,096	2018-11-02 18:46:49	2018-10-25 16:09:03	2018-11-02 18:46
11	desktop.ini		ini	432	2018-10-25 16:09:00	2018-10-25 16:09:00	2018-10-25 16:09
12	document.lnk		lnk	412	2018-10-31 11:44:22	2018-10-31 11:44:22	2018-10-31 11:44
13	InvoiceTemplate.lnk		lnk	579	2018-10-31 11:44:22	2018-10-31 11:44:22	2018-10-31 11:44
14	InvoiceTemplate2.lnk		lnk	2,338	2018-10-31 11:44:58	2018-10-31 11:44:58	2018-10-31 11:44
15	PA2018.lnk		lnk	612	2018-11-01 11:56:33	2018-11-01 11:56:33	2018-11-01 11:56
16	request for quotation.lnk		lnk	632	2018-11-01 14:51:25	2018-10-29 15:11:43	2018-11-01 14:51
17	victor_PC_memdump.dmp.lnk		lnk	372	2018-11-02 18:31:09	2018-11-02 18:31:09	2018-11-02 18:31
18	下载.lnk		lnk	435	2018-11-01 11:56:33	2018-11-01 11:56:33	2018-11-01 11:56
19	可移动磁盘 (F).lnk		lnk	219	2018-11-02 18:31:09	2018-11-02 18:31:09	2018-11-02 18:31
20	图片.lnk		lnk	589	2018-11-02 14:36:38	2018-10-31 11:50:31	2018-11-02 14:36
21	我的图片.lnk		lnk	1,312	2018-10-31 11:51:45	2018-10-31 11:51:45	2018-10-31 11:51
22	捕获.lnk		lnk	534	2018-10-30 11:03:35	2018-10-29 19:24:00	2018-10-30 11:03
23	教师学位化　教局拟中学一次过小学分阶段实施...		lnk	1,893	2018-11-01 11:50:43	2018-11-01 11:50:43	2018-11-01 11:50
24	教育局局长出席甬港教育合作论坛致辞全文 (...		lnk	2,547	2018-11-01 11:52:27	2018-11-01 11:52:27	2018-11-01 11:52
25	文档.lnk		lnk	592	2018-11-01 11:50:43	2018-11-01 11:50:43	2018-11-01 11:50
26	毛笔.lnk		lnk	534	2018-11-02 11:17:10	2018-11-01 16:48:32	2018-11-02 11:17
27	消息：教師學位化兩至三年內全面落實 - Now...		lnk	2,668	2018-11-01 11:56:14	2018-11-01 11:56:14	2018-11-01 11:56

27. 接上题，""的元数据(metadata)记录了以下哪个网卡的物理地址(mac address)? (2分)

A. 00:0C:29:70:F4:47

B. 00:50:56:C0:00:13

C. 47:F4:70:29:0C:00

D. E4:A7:A0:CB:66:C7

E. 00:0C:29:70:F4:47

解析：以“request for quotation.lnk”为关键词搜索，可得答案

序号	名称	快捷文件全路径	目标文件	MAC地址	创建时间	修改时间
26	PA2018.lnk	分区3_本地磁盘[E]:\Users\victor\AppData\Roam...	C:\Users\victor\Downloa...	E4:A7:A0:CB:6...	2018-11-01 11:56...	2018-11-01 11:56...
27	Price-Quotation-Template-Excel-Free-D...	分区3_本地磁盘[E]:\Users\Lily\AppData\Roamin...	F:\document\Price-Quo...	E4:A7:A0:CB:6...	2018-10-30 12:20...	2018-10-30 12:20...
28	QQ音乐.lnk	分区3_本地磁盘[E]:\Users\Public\Desktop\QQ音...	C:\Program Files (x86)\Te...	E4:A7:A0:CB:6...	2018-10-29 13:44...	2018-08-01 14:44...
29	Reddy Resume.lnk	分区3_本地磁盘[E]:\Users\simon\AppData\Roam...	C:\Users\simon\Downloa...	E4:A7:A0:CB:6...	2018-10-31 08:28...	2018-10-31 08:28...
30	request for quotation.lnk	分区3_本地磁盘[E]:\Users\victor\AppData\Roami...	C:\Users\victor\Desktop...	E4:A7:A0:CB:6...	2018-10-29 15:11...	2018-10-29 15:11...
31	SampleJobApplicationForm.lnk	分区3_本地磁盘[E]:\Users\simon\AppData\Roam...	C:\Users\simon\Downloa...	E4:A7:A0:CB:6...	2018-10-31 08:32...	2018-10-31 08:32...
32	ug.lnk	分区3_本地磁盘[E]:\Users\Lily\AppData\Roamin...	F:\document\ug.jpeg	E4:A7:A0:CB:6...	2018-10-30 12:17...	2018-10-29 12:38...
33	Uninstall WPS Office.lnk	分区3_本地磁盘[E]:\Users\victor\AppData\Roami...	C:\Users\victor\AppData...	E4:A7:A0:CB:6...	2018-10-29 14:59...	2018-10-29 14:59...
34	Uninstall.lnk	分区3_本地磁盘[E]:\Users\victor\AppData\Roami...	C:\Users\victor\AppDat...	E4:A7:A0:CB:6...	2018-10-30 11:04...	2018-10-30 11:04...
35	WhatsApp Image 2018-09-11 at 17.23.4...	分区3_本地磁盘[E]:\Users\Lily\AppData\Roaming...	F:\document\WhatsApp ...	E4:A7:A0:CB:6...	2018-10-30 12:17...	2018-09-11 17:24...
36	WPS 2019.lnk	分区3_本地磁盘[E]:\Users\Lily\AppData\Roamin...	C:\Program Files (x86)\W...	E4:A7:A0:CB:6...	2018-10-30 12:37...	2018-10-30 12:37...
37	WPS 2019.lnk	分区3_本地磁盘[E]:\Users\Lily\Desktop\WPS 201...	C:\Program Files (x86)\W...	E4:A7:A0:CB:6...	2018-10-30 12:37...	2018-10-30 12:37...
38	WPS H5.lnk	分区3_本地磁盘[E]:\Users\simon\AppData\Roam...	C:\Users\simon\AppDat...	E4:A7:A0:CB:6...	2018-10-31 08:31...	2018-10-31 08:31...
39	WPS Office Configuration Tools.lnk	分区3_本地磁盘[E]:\Users\victor\AppData\Roami...	C:\Users\victor\AppDat...	E4:A7:A0:CB:6...	2018-10-29 14:59...	2018-10-29 14:59...
40	WPS Presentation.lnk	分区3_本地磁盘[E]:\Users\victor\AppData\Roam...	C:\Users\victor\AppDat...	E4:A7:A0:CB:6...	2018-10-29 14:59...	2018-10-29 14:59...

28. 系统账号victor使用以下哪个电子邮件发送/接收的程序? (2分)

A. Outlook express

B. Lotus Note

C. Thunderbird

D. Roundcube

E. 没有安装以上软件

解析：取证大师直接分析得出

29. 系统经哪个IP地址，登录互联网？ (2分)

A. 10.0.4.1

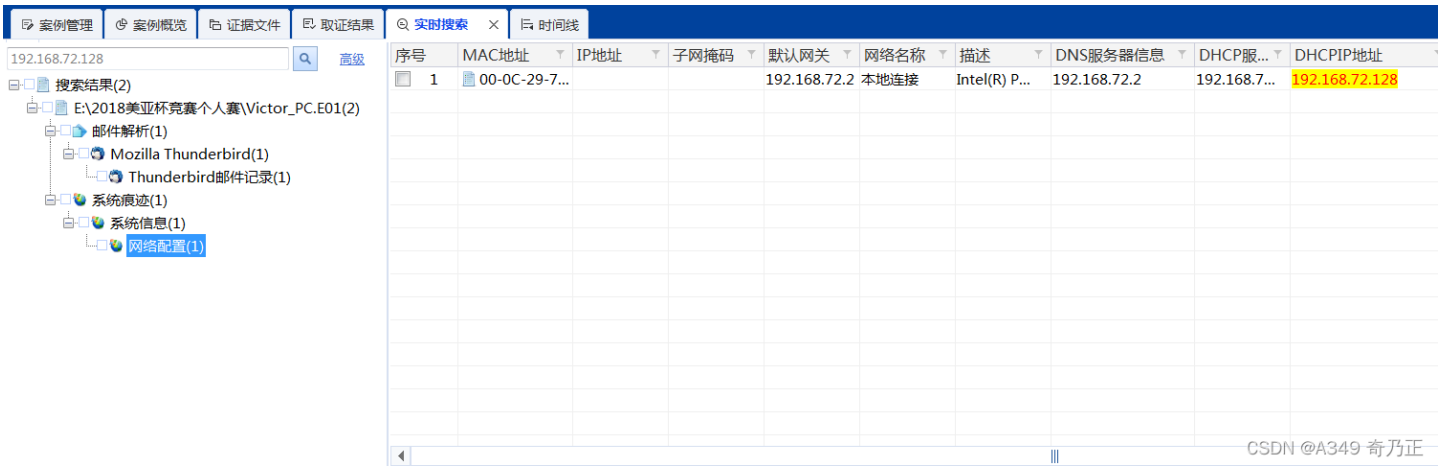
B. 10.0.4.128

C. 192.168.72.2

D. 192.168.72.128

E. 192.168.72.233

解析：对选项进行搜索可得答案



30. 在该操作系统中，曾经连接数个USB移动储存装置
(U盘)，下列那个是该系统连接过的USB移动储存装置？(2分)

A. Verbatim USB Device

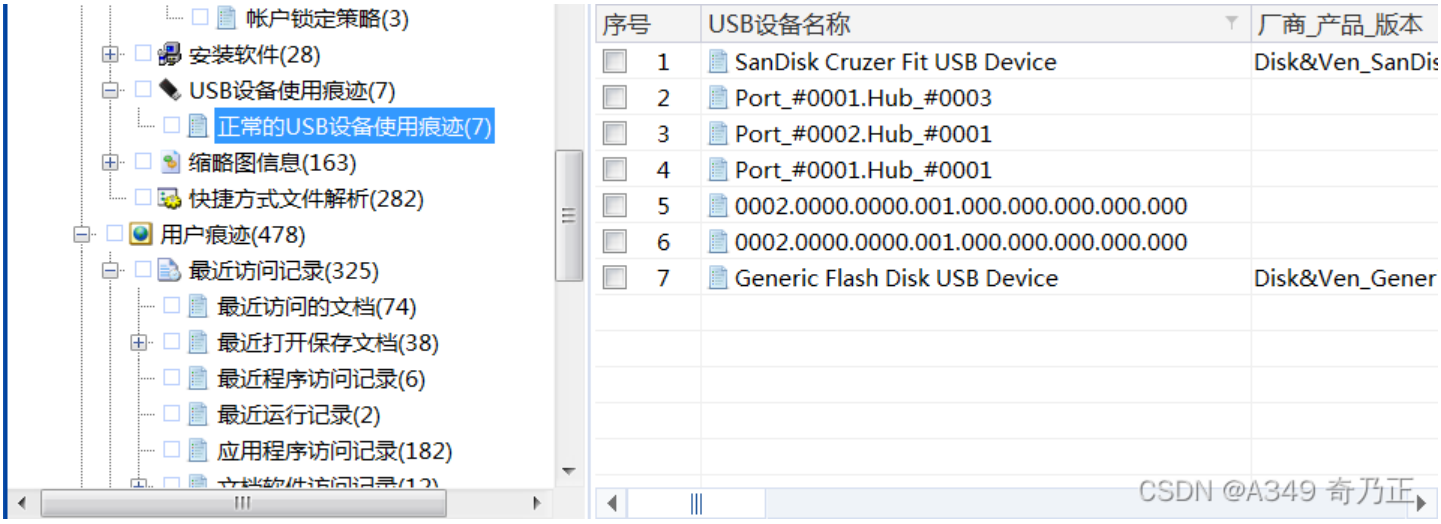
B. USB Mass storage USB Device

C. WD 2500BMV External USB Device

D. SanDisk Cruzer Fit USB Device

E. Seagate 250 External USB Device

解析：取证大师直接分析得出



31. 在操作系统中，上述U盘曾被指派以下哪个磁盘分区代号(Drive Letter)？(2分)

A. D:

B. E:

C. F:

D. G:

E. Z:

解析：取证大师直接分析得出

序号	USB设备名称	厂商_产品_版本	首次插拔时间	最后插拔时间	最后一次启动的首次...	挂载盘符	系统用户	设备描述	设备
1	SanDisk Cruzer Fit USB Device	Disk&Ven_SanDisk&Pro...	2018-11-02 18:30...	2018-11-02 18:30...	2018-11-02 18:30:23	F:	victor	USB 大容量存储设备	4C53
2	Port_#0001.Hub_#0003		2018-10-29 13:00...	2018-11-02 18:22...	2018-11-02 18:22:56			Generic Bluetooth Adap...	0006
3	Port_#0002.Hub_#0001		2018-10-25 16:04...	2018-11-02 18:22...	2018-11-02 18:22:55			Generic USB Hub	6&b7
4	Port_#0001.Hub_#0001		2018-10-25 16:04...	2018-11-02 18:22...	2018-11-02 18:22:55			USB Composite Device	6&b7
5	0002.0000.0000.001.000.000.000.000.000		2018-10-25 16:04...	2018-11-02 18:22...	2018-11-02 18:22:55			USB 输入设备	7&2a
6	0002.0000.0000.001.000.000.000.000.000		2018-10-25 16:04...	2018-11-02 18:22...	2018-11-02 18:22:55			USB 输入设备	7&2a
7	Generic Flash Disk USB Device	Disk&Ven_Generic&Pro...	2018-10-30 12:31...	2018-10-31 11:44...	2018-10-31 11:44:08		victor	USB 大容量存储设备	E676

2018-11-02 18:22:56

32. 该操作系统中，下列哪个是最后的关机时间？（答案格式一“世界协调时间 "：YYYY-MM-DD HH:MM:SS UTC） (2分)

A. 2018-11-02 08:59:38 UTC

B. 2018-11-02 10:22:40 UTC

C. 2018-11-02 10:23:03 UTC

D. 2018-11-02 10:47:28 UTC

E. 2018-11-02 10:47:51 UTC

解析：取证大师直接分析得出

序号	名称	值	系统
7	注册所有者	victor	Windows 7 Professional
8	当前版本	6.1	Windows 7 Professional
9	当前Build版本	7601	Windows 7 Professional
10	最新服务包	Service Pack 1	Windows 7 Professional
11	系统根路径	C:\Windows	Windows 7 Professional
12	源路径		Windows 7 Professional
13	路径名	C:\Windows	Windows 7 Professional
14	产品ID	00371-177-0000061-85...	Windows 7 Professional
15	操作系统类型	64位	Windows 7 Professional
16	最后一次正常关...	2018-11-02 18:47:51	Windows 7 Professional
17	制造商		Windows 7 Professional
18	型号		Windows 7 Professional

33. 该操作系统中，下列哪个是计算机的主机名？(2分)

A. VICTOR-COMPUTER

B. WORKGROUP

C. SIMON-HOME

D. VICTOR-HOME

E. LILY-HOME

解析：取证大师直接分析得出

序号	名称	值	系统
1	完整计算机名	VICTOR-HOME	Windows 7 Profe
2	工作组	WORKGROUP	Windows 7 Profe
3	计算机描述		Windows 7 Profe
4	安装时间	2018-10-25 16:08:39	Windows 7 Profe
5	产品名称	Windows 7 Professional	Windows 7 Profe
6	注册组织		Windows 7 Profe
7	注册所有者	victor	Windows 7 Profe
8	当前版本	6.1	Windows 7 Profe
9	当前Build版本	7601	Windows 7 Profe
10	最新服务包	Service Pack 1	Windows 7 Profe
11	系统根路径	C:\Windows	Windows 7 Profe
12	源路径		Windows 7 Profe

34. 接上题，设定为上述计算机主机名前是什么名称? (2分)

A. 42P323K467-22

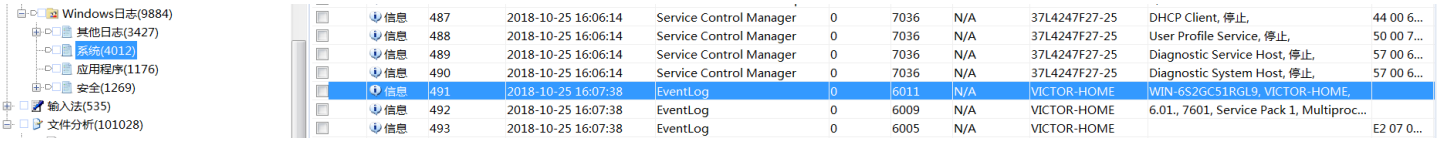
B. 37L4247F27-25

C. WIN-6S2GC51RGL9

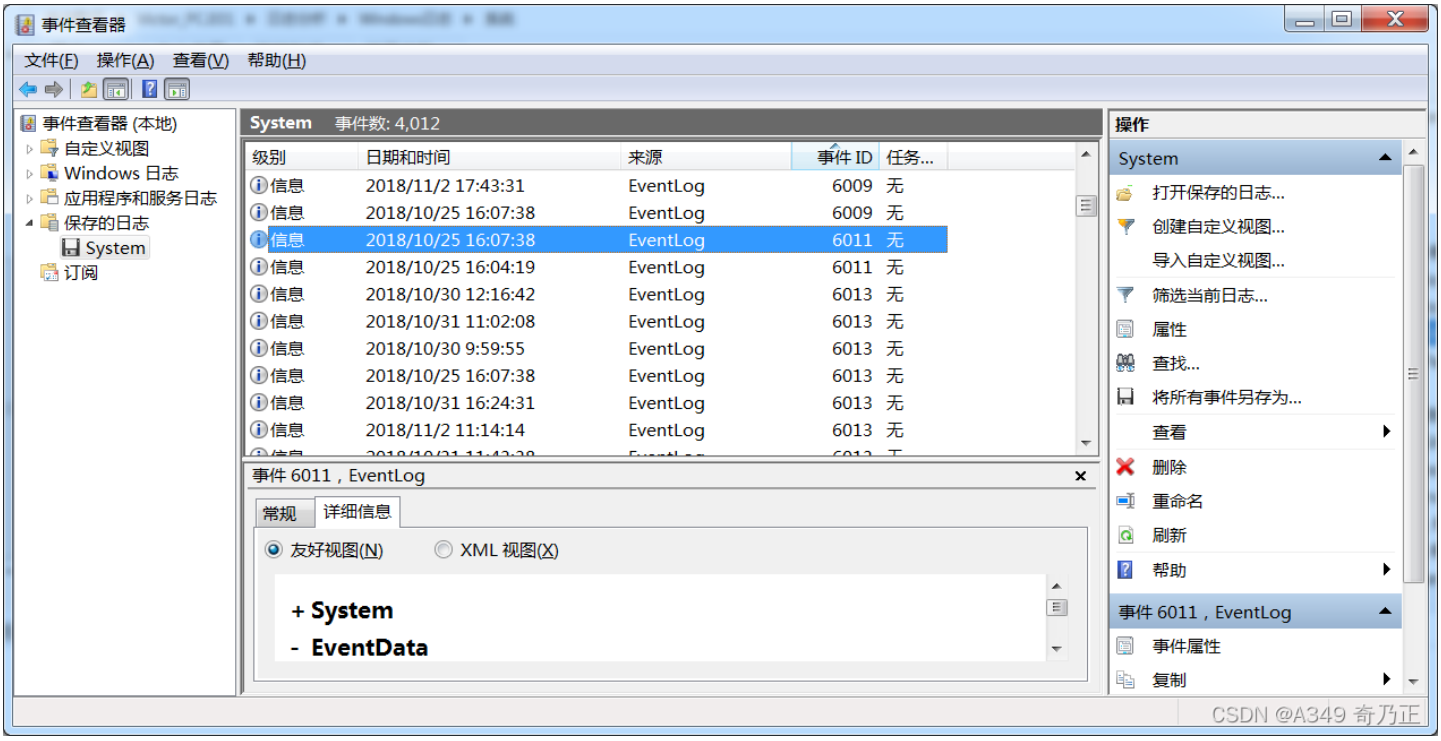
D. USER-PC

E. MY-PC

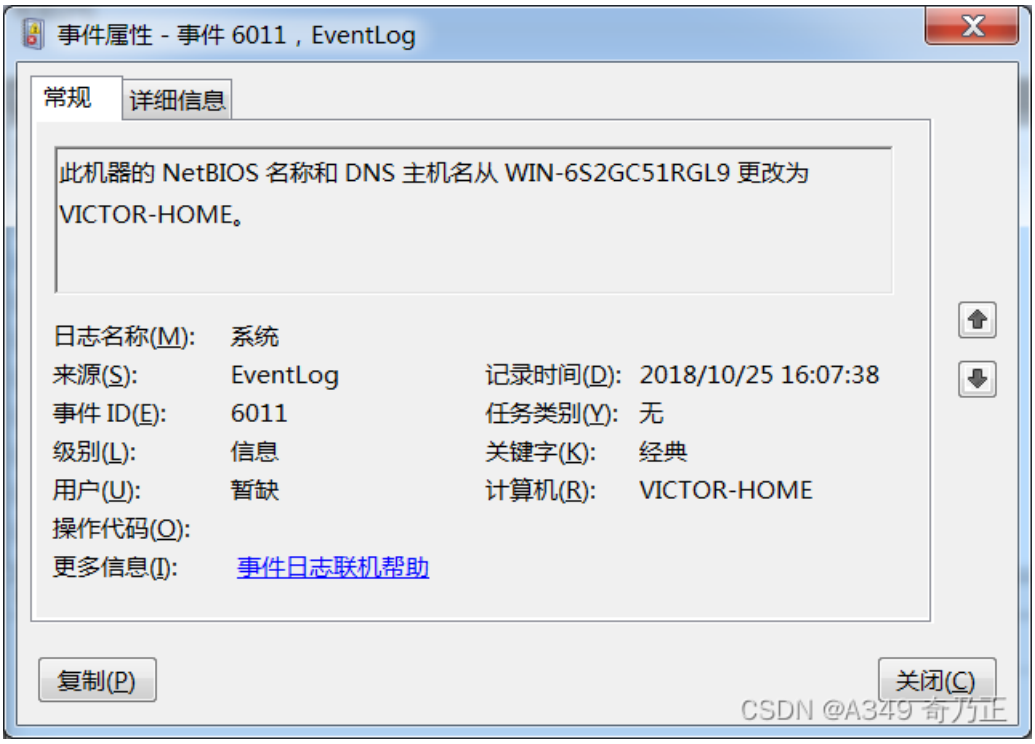
解析：第一步：查看系统日志，发现有主机名做更改的日志



第二步：跳转并打开相应文件，按照事件ID查找事件



第三步：查看事件详情。



35. 接上题，上述计算机主机名设定时间是？（答案格式 一“本地时间 " ：YYYY-MM-DD HH:MM:SS +8） (2分)

A. 2018-10-24 11:07:22 +8

B. 2018-10-28 12:22:59 +8

C. 2018-10-27 13:45:18 +8

D. 2018-10-25 16:04:19 +8

E. 2018-10-25 16:07:38 +8

解析：如上题图：记录时间项

36. 在该操作系统中，下列哪个是用户victor日常使用的电邮账号? (2分)

A. victor201811@hotmail.com

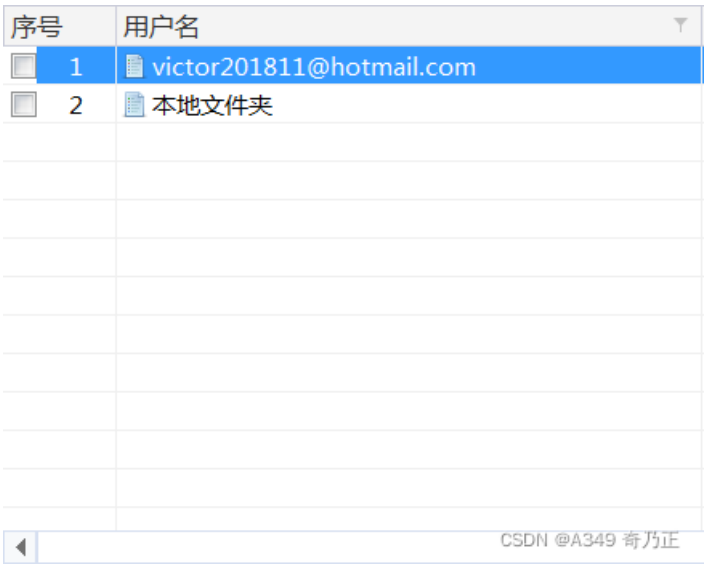
B. wictor2018111@hotmail.com

C. victor_201811@google.com

D. victorlam2018@hotmail.com

E. 以上皆不是

解析：取证大师直接分析得出



37. victor 上一次更改上述电邮账号密码是什么时候？（答案格式一“本地时间 "：YYYY-MM-DD） (2分)

A. 2018-10-29

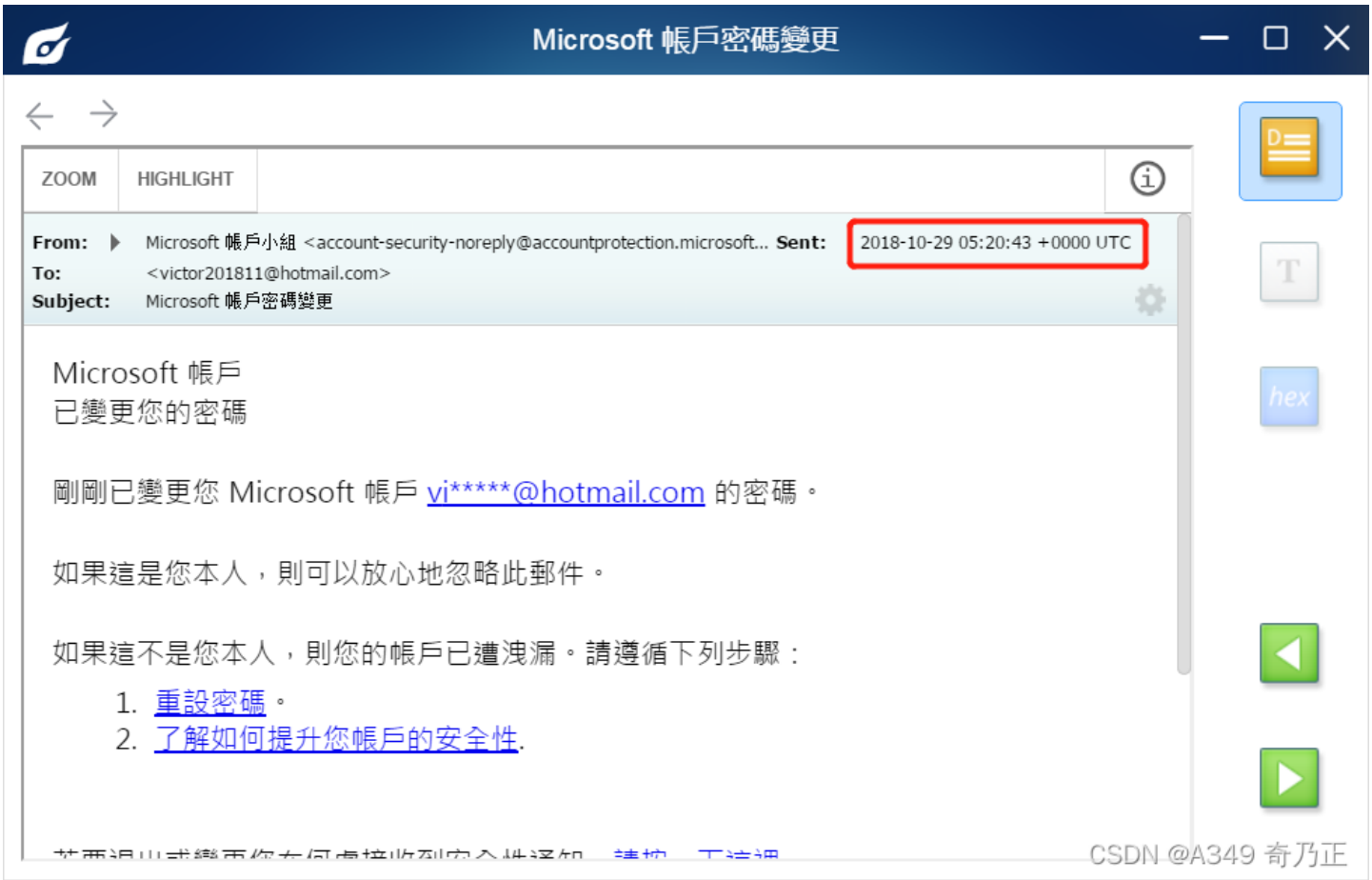
B. 2018-10-30

C. 2018-10-31

D. 2018-11-01

E. 2018-11-02

解析：查看电子邮件详细信息可得答案。



38. victor什么时候收到勒索电邮？（答案格式 一“本地时间 " ：YYYY-MM-DD HH:MM +8）
(2分)

A. 2018-11-02 09:09 +8

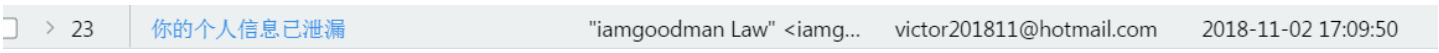
B. 2018-11-02 09:10 +8

C. 2018-11-02 10:09 +8

D. 2018-11-02 17:09 +8

E. 2018-11-02 17:10 +8

解析：找到相关邮件可得时间



39. 以下哪个是发出勒索邮件的的IP地址? (2分)

A. 10.152.64.57

B. 10.152.64.217

C. 220.246.55.13

D. 74.208.4.220

E. 10.76.45.13

解析：找到相关邮件可得IP地址

40. 勒索邮件的附件解压后有一个病毒文件，这个文件的MD5哈希值是? (2分)

A. 72596F71248531853F37D4BD15D088C4

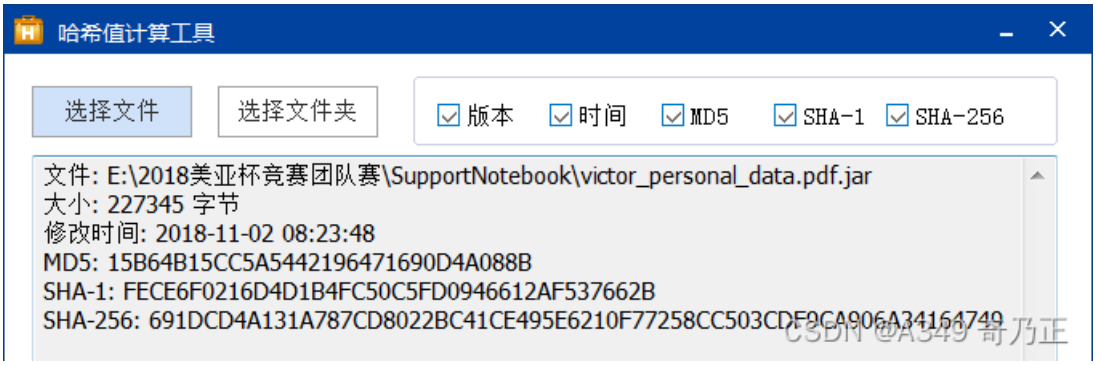
B. 15B64B15CC5A5442196471690D4A088B

C. 67A1487E296328C9E802D50741D8DB9C

D. 72596F71248DH3S92LS7D4BD15D088C4

E. 5BB71EF8E95A5249EF4C2A8CFF9A1E1C

解析：找到文件解压后计算MD5值



41. 上述的病毒文件什么时间被系统执行？（答案格式 一“本地时间 " ：YYYY-MM-DD HH:MM +8） (2分)

A.2018-11-02 14:15 +8

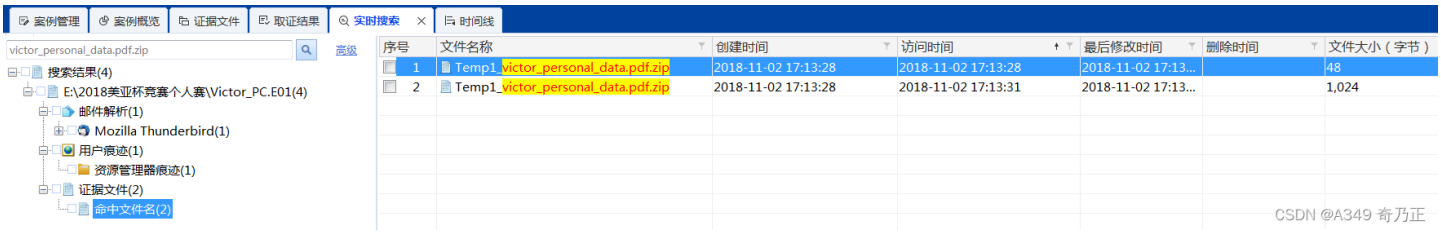
B.2018-11-02 17:09 +8

C.2018-11-02 17:13 +8

D.2018-11-02 17:20 +8

E.2018-11-02 17:23 +8

解析：搜索文件，可得其最早访问时间



42. 这个病毒是否会在重新开机后自动运行?如会，它是通过下列哪个程序执行? (2分)

A. Thunder.exe

B. QyKernel.exe

C. QyClient.exe

D. javaw.exe

E. 病毒不会自动执行

解析：解压后发现是个jar程序，判断通过javaw.exe运行

43. 病毒文件被执行后有以下哪个文件被生成? (2分)

A. E8S377N3N8UOAMS82PQJ.temp

B. tbc_stat_cache.dat

C. JNativeHook_4940080920928265976.dll

D. 83aa4cc77f591dfc2374580bbd95f6ba.tmp

E. downloads.json

解析：通过反编译发现里边只有两个.class文件，估计占用空间也就十几K，可是jar包却要200多K，但是怎么分析能够得到生成的文件我还没找到，如果个人赛现场开虚拟机用动态分析运行监控的话，太浪费时间了，并且不一定能找到答案。此题不会。

44. 接上题，上述文件有什么功能? (2分)

A. 获取镜头权限

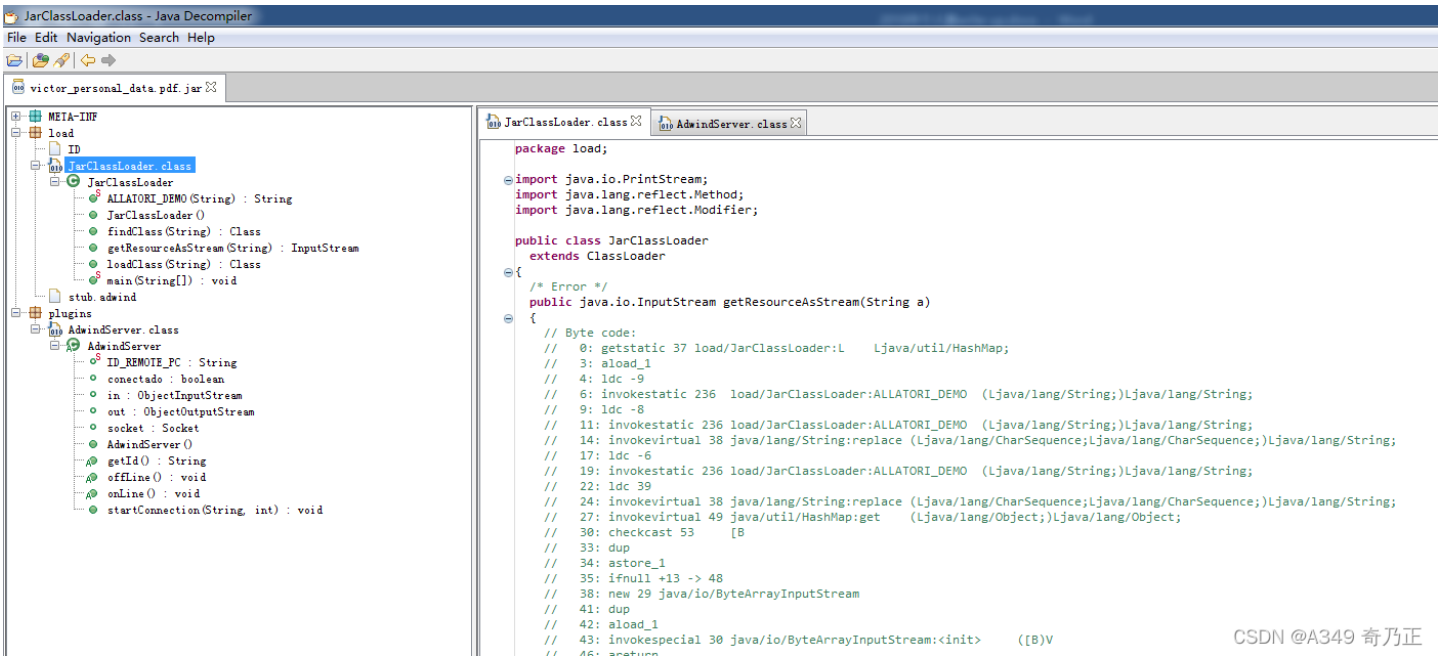
B. 追踪键盘记录

C. 抓取浏览器密码

D. 抓取系统登入密码

E. 存取系统分区

解析：使用JDGUI进行反编译，通过读java代码得出



45. 以下哪个是系统安装的第三方输入法软件? (2分)

A. sogou pinyin

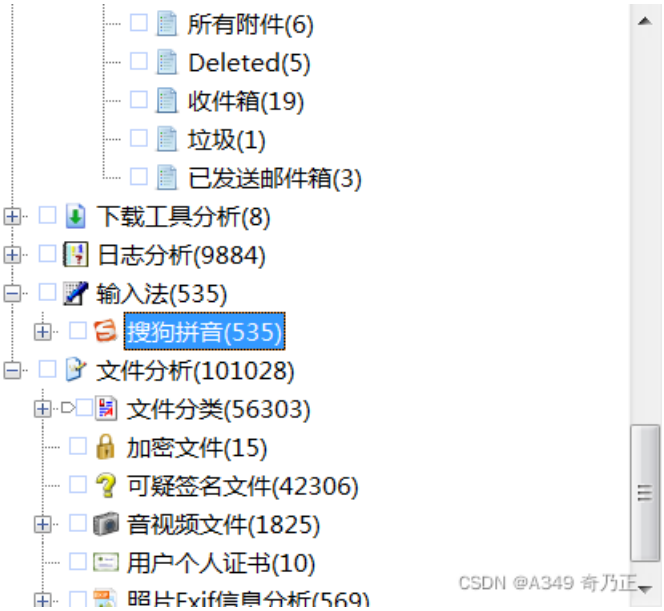
B. sogou wubi

C. Baidu Pinyin

D. QQ Pingyin

E. 以上皆不是

解析：取证大师直接分析得出



46. 操作系统是跟哪一个时间服务器自动同步? (2分)

A. time.nist.gov

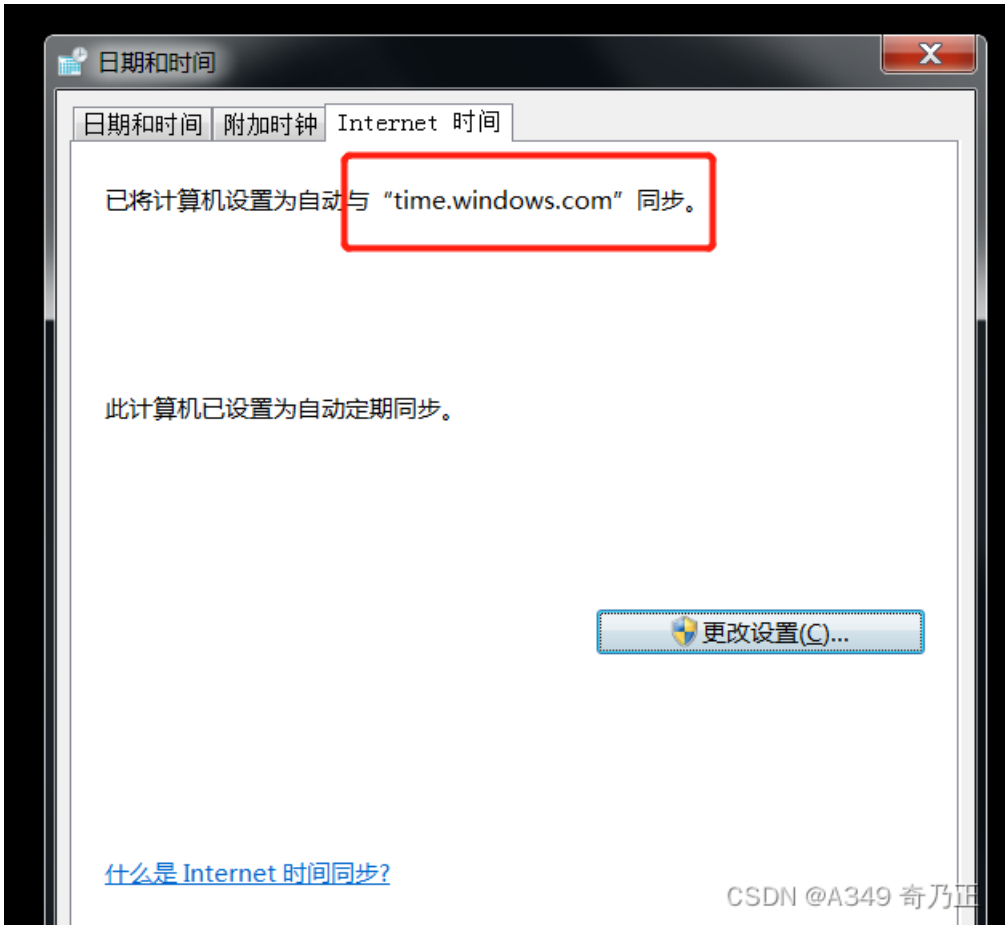
B. time-a.nist.gov

C. time.windows.com

D. time-b.nist.gov

E. time-nw.nist.gov

解析：在仿真系统中，找到时间设置即可



47. 法证人员于2018-11-02 下午6时25分到场，之后对系统作以下哪项取证? (2分)

A. 抓取荧幕画面

B. 备份使用者资料

C. 备份浏览记录

D. 抓取网络数据包

E. 制作内存镜像档

解析：由48题可得。

48. 法证人员到场后，以下哪个软件曾经在系统里运行过? (2分)

A. wireshark.exe

B. Magnet RAM capture.exe

C. Lightscreen.exe

D. fastdump.exe

E. 以上皆不是

解析：由49题可得

49. 接上题，所抓取的资料被储存为以下哪个文件? (2分)

A. victor_PC_networktraffic.pcapng

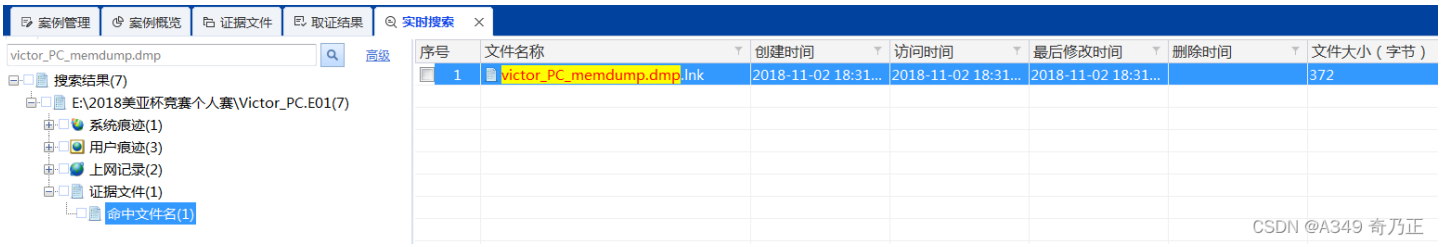
B. Lily_PC.networktraffice.pcapng

C. PC_ screenshot.PNG

D. victor_PC_memdump.dmp

E. Lily_PC_memdump.dmp

解析：搜索选项可得



50. 接上题，上述档案储存到以下哪个分区? (2分)

A. D：

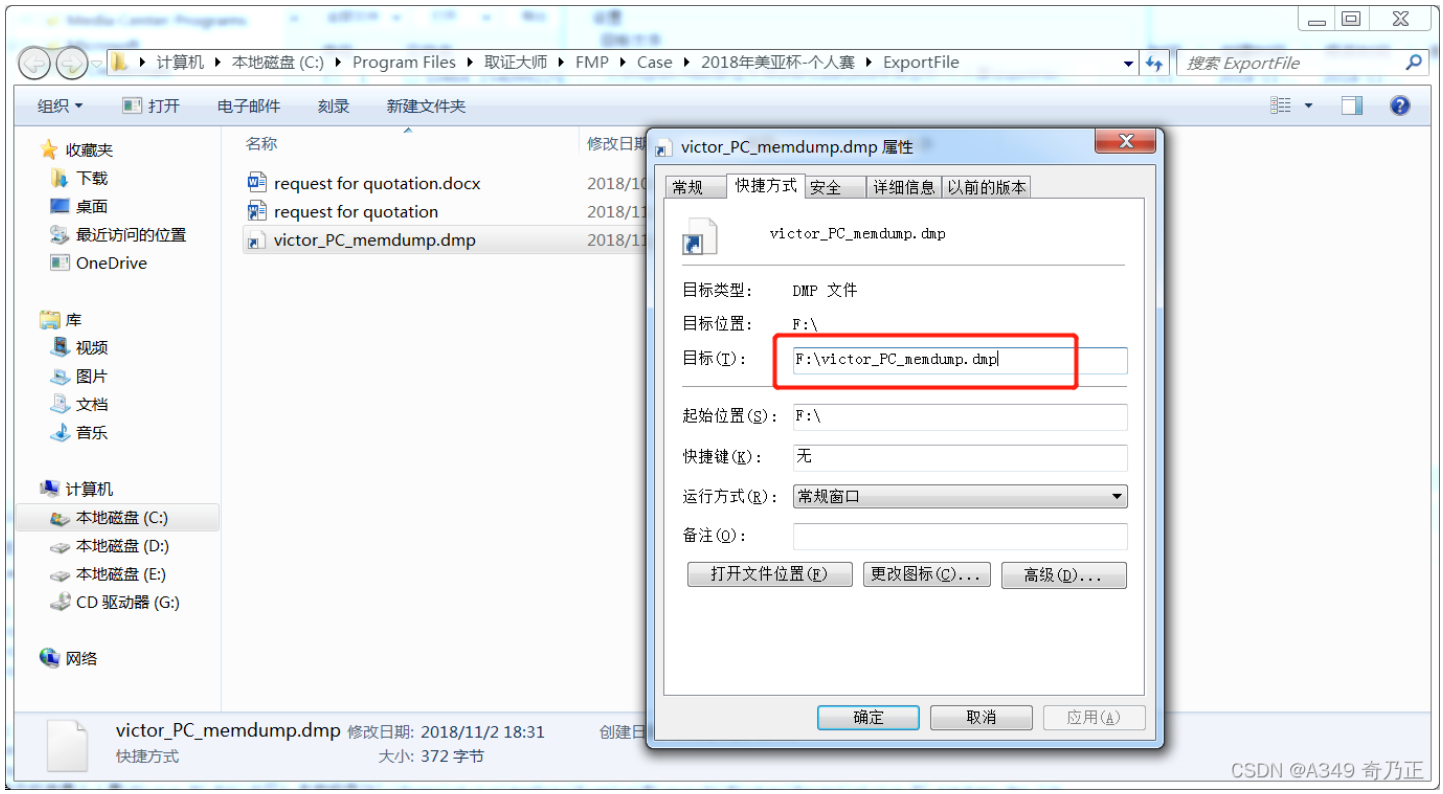
B. E：

C. F:

D. G:

E. H:

解析：导出快捷方式，查看属性-目标。


计算机 ▸ 本地磁盘 (C:) ▸ Program Files ▸ 取证大师 ▸ FMP ▸ Case ▸ 2018年美亚杯-个人赛 ▸ ExportFile
搜索 ExportFile
组织
打开
电子邮件
刻录
新建文件夹
收藏夹
下载
桌面
最近访问的位置
OneDrive
库
视频
图片
文档
音乐
计算机
本地磁盘 (C:)
本地磁盘 (D:)
本地磁盘 (E:)
CD 驱动器 (G:)
网络
名称
修改日期
request for quotation.docx
request for quotation
victor_PC_memdump.dmp
victor_PC_memdump.dmp 属性
常规
快捷方式
安全
详细信息
以前的版本
victor_PC_memdump.dmp
目标类型: DMP 文件
目标位置: F:\
目标(T): F:\victor_PC_memdump.dmp
起始位置(S): F:\
快捷键(K): 无
运行方式(R): 常规窗口
备注(O):
打开文件位置(F)
更改图标(C)...
高级(D)...
确定
取消
应用(A)
victor_PC_memdump.dmp 修改日期: 2018/11/2 18:31
快捷方式
大小: 372 字节
CSDN @A349 奇乃正