2017第三届美亚杯全国电子数据取证大赛团队赛write up

原创

奇乃正 于 2022-01-02 21:52:41 发布 2414 收藏 1
分类专栏： 电子数据取证 网络安全 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/122281025
版权


电子数据取证 同时被 3 个专栏收录

6 篇文章 3 订阅
订阅专栏


网络安全

5 篇文章 1 订阅
订阅专栏


取证

5 篇文章 2 订阅
订阅专栏

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

Gary被逮捕后,其计算机被没收并送至计算机取证实验室。经调查后，执法机关再逮捕一名疑犯Eric，并检取其家中计算机(window
8), 并而根据其家中计算机纪录,
执法机关再于其他地方取得一台与案有关的服务器,而该服务器内含四个硬盘。该服务器是运行LINU√
系统。

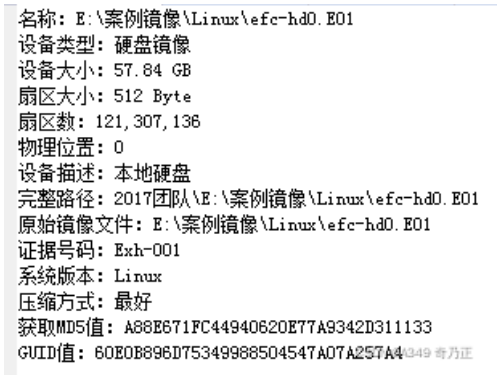
由于事件涉及Windows 7,8, LINUX及Mac
IOS系统，故取证团队有可能需要使用相关系统之取证工具(105题,105分)

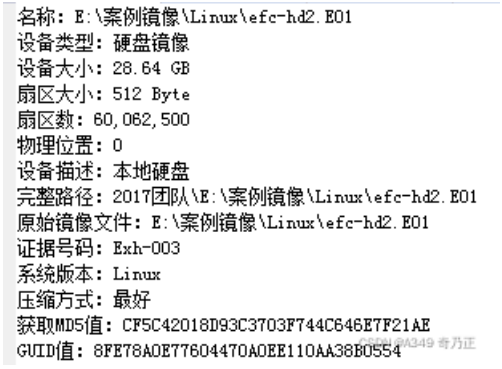
E01 Images

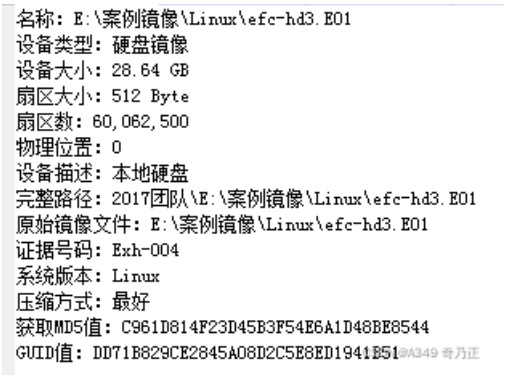
	1	被检取作法证检验的LINUX系统，共有四个硬盘，已经分别被制作为四个E01法证镜像文件(Forensic Images)，下列哪个不是它们的MD5哈希值(Hash value)?
	A.	2e4a6afe6b27188480d1b7b10e576f7c
√	B.	c961d814f99d45b3f54e8a1d48be8544
	C.	a88e671fc44940620e77a9342d311133
	D.	c961d814f23d45b3f54e6a1d48be8544
	E.	cf5c42018d93c3703f744c646e7f21ae

答案：B. c961d814f99d45b3f54e8a1d48be8544

解答：





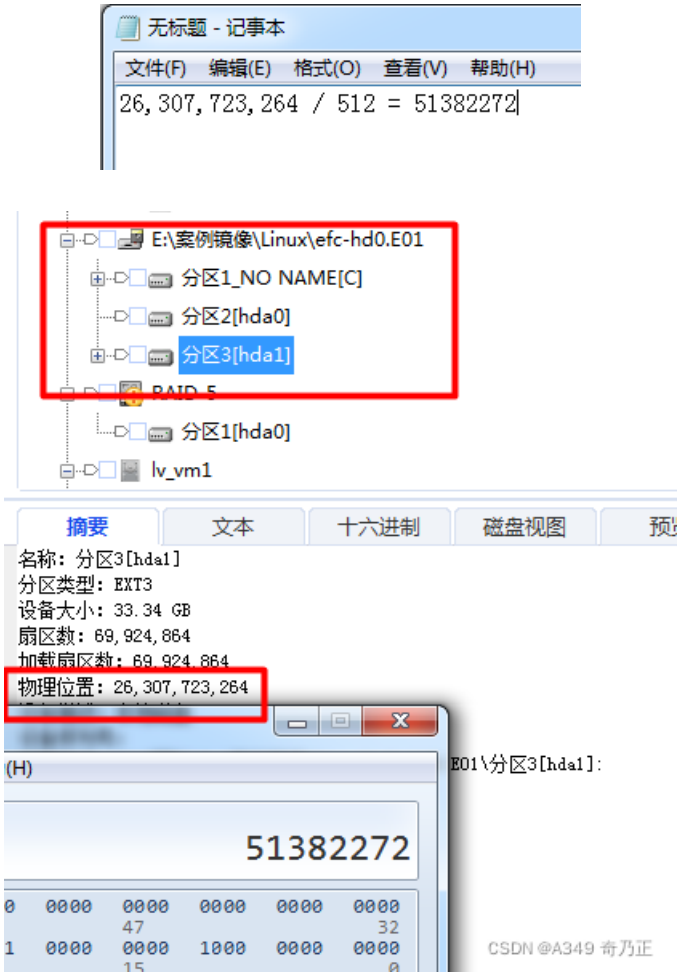


	2	**上述四个法证镜像文件中，其中有一个法证镜像文件(Forensic Image)内含三个磁盘分区(Partition)。对于第三个(即最后一个)磁盘分区(Partition)而言，下列哪个是其起始磁区(Starting Sector)?**
	A.	2048
	B.	1050624
	C.	51382271
√	D.	51382272

	2	上述四个法证镜像文件中，其中有一个法证镜像文件(Forensic Image)内含三个磁盘分区(Partition)。对于第三个(即最后一个)磁盘分区(Partition)而言，下列哪个是其起始磁区(Starting Sector)?
	E.	50331648

答案：D. 51382272

解答：



	3	上述磁盘分区(Partition)共占多少磁区(Starting Sector)?
√	A.	69924864
	B.	60058404
	C.	50331648
	D.	1048576
	E.	2048

答案：A. 69924864

解答：

	4	在上述第三个(即最后一个)磁盘分区(Partition)当中，储存了一个名为amons.mark的文件，下列哪项为其MD5哈希值(Hash value)
	A.	01daa9fb8d1cc386bffb0c25ff57d7ea
	B.	64394febb8fb82520164645ade7dbaa0
	C.	b69894efe2f03d43d95d98856ea21674
	D.	74c5d7a6500d63a0308f2fc54a03eb0d
√	E.	43309465540a069357182af1da438a07

答案：E. 43309465540a069357182af1da438a07

解答：

	5	在上述第三个(即最后一个)磁盘分区(Partition)当中，储存了一个名为slackware-13.37-install-dvd.iso的文件，下列哪项为其MD5哈希值(Hash value)
	A.	01daa9fb8d1cc386bffb0c25ff57d7ea
√	B.	64394febb8fb82520164645ade7dbaa0
	C.	b69894efe2f03d43d95d98856ea21674
	D.	74c5d7a6500d63a0308f2fc54a03eb0d
	E.	43309465540a069357182af1da438a07

答案：B. 64394febb8fb82520164645ade7dbaa0

解答：

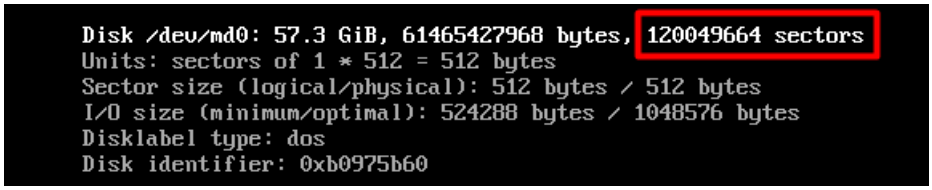
VM-HD1,2,3

RAID

	6	于上述四个法证镜像文件中，有三个硬盘共同组成一个独立磁盘冗余阵列RAID System。以磁区(sector)计算，该阵列(RAID)大小(size)是多少？
	A.	110051100
	B.	110049052
	C.	110049053
√	D.	120049664
	E.	120049663

答案：D. 120049664

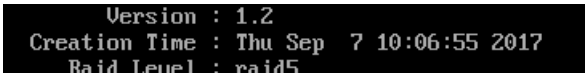
解答：



	7	就该独立磁盘冗余阵列RAID System而言，下列哪项是其建立日期？
	A.	2017-09-05 10:06:55
	B.	2017-09-06 10:06:55
√	C.	2017-09-07 10:06:55
	D.	2017-09-08 10:06:55
	E.	2017-09-08 10:06:55

答案: C. 2017-09-07 10:06:55

解答：



	8	就该独立磁盘冗余阵列RAID System而言，下列哪项是其UUID?

	8	就该独立磁盘冗余阵列RAID System而言，下列哪项是其UUID?
	A.	ae891891:ab1261bf:17f4b1e8:c1adaef6
	B.	ae891891:ac1261bf:27f4b1e8:c1adaef6
√	C.	ae891891:ad1261bf:37f4b1e8:c1adaef6
	D.	ae891891:ae1261bf:57f4b1e8:c1adaef6
	E.	ae891891:af1261bf:67f4b1e8:c1adaef6

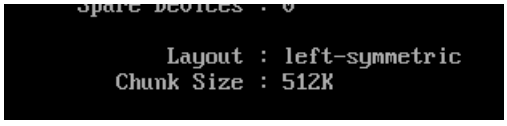
答案：C. ae891891:ad1261bf:37f4b1e8:c1adaef6

解答：

	9	就该独立磁盘冗余阵列RAID System而言，是使用了下列哪种阵列配置排列(RAID LAYOUT)?
√	A.	left-symmetric
	B.	right-symmetric
	C.	pre-Lie algebra
	D.	rooted tree algebras
	E.	verte√ algebras

答案：A. left-symmetric

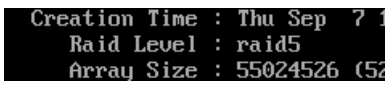
解答：



	10	就该独立磁盘冗余阵列RAID System而言，是使用了下列哪种阵列级别(RAID LEVEL)?
	A.	RAID 0
	B.	RAID 1
√	C.	RAID 5
	D.	RAID 6
	E.	RAID 1 0

答案：C. RAID 5

解答：



LVM

	11	此外，在该独立磁盘冗余阵列RAID System中，内含一个标示为逻辑分卷管理器Logical Volume Manager (LVM) 的磁盘分区(Partition)，此分区(Partition)共有多少个磁区(Sector)?
	A.	110051100
	B.	110049052
√	C.	110049053
	D.	120049664
	E.	120049663

答案：C. 110049053

解答：

	12	就上述逻辑分卷管理器Logical Volume Manager (LVM)而言，下列哪个是其仅有的物理卷Physical Volume (PV) UUID？
	A.	l87QVT-6ljH-bVea-dM3H-OMtA-2y0l-yitBi9
√	B.	ysHo03-FFL9-0Tfl-zOeO-O7fn-TPz√-2p4mu0
	C.	UGpPyJ-lSUZ-eGJh-hrny-qPFY-UFUA-DfZ8mw
	D.	eSpqp3-OwnF-9ari-aEKV-ljRq-KjcY-kLz5Ul
	E.	UGpPyJ-lSUZ-eGJh-aEKV- OMtA-2y0l-yitBi9

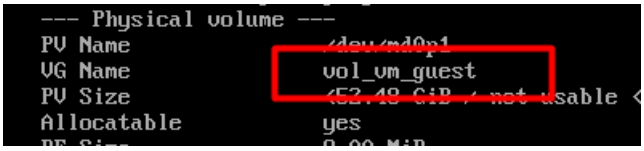
答案：B. ysHo03-FFL9-0Tfl-zOeO-O7fn-TPz√-2p4mu0

解答：

	13	在该物理卷Physical Volume (PV)中，下列哪个是其仅有的卷组 Volume Group (VG) 名称？
	A.	vol_vm_guests
√	B.	vol_vm_guest
	C.	vol_guest
	D.	lv_vm1
	E.	lv_vm2

答案：B. vol_vm_guest

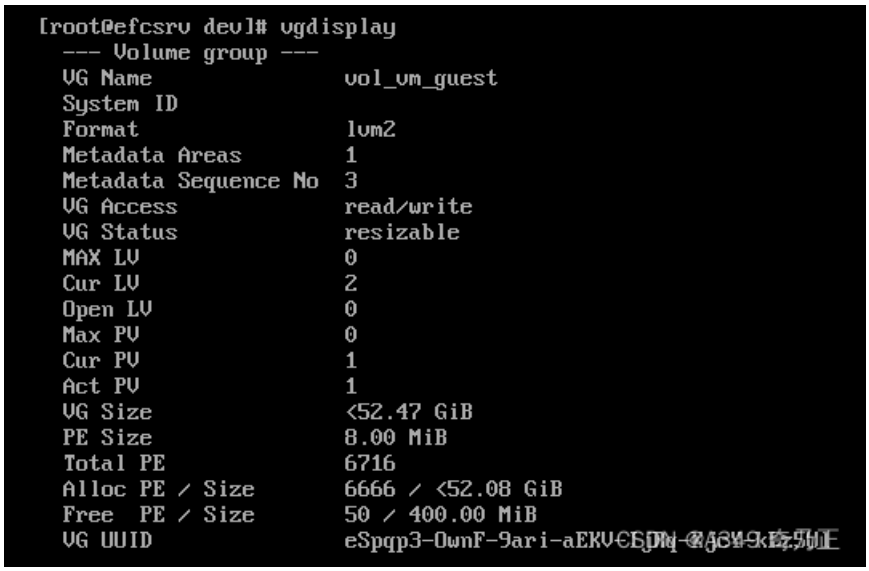
解答：



	14	**下列哪项是该卷组 Volume Group (VG) UUID ?**
	A.	l87QVT-6ljH-bVea-dM3H-OMtA-2y0l-yitBi9
	B.	ysHo03-FFL9-0Tfl-zOeO-O7fn-TPz√-2p4mu0
	C.	UGpPyJ-ISUZ-eGJh-hrny-qPFY-UFUA-DfZ8mw
√	D.	eSpqp3-OwnF-9ari-aEKV-ljRq-KjcY-kLz5Ul
	E.	UGpPyJ-ISUZ-eGJh-aEKV- OMtA-2y0l-yitBi9

答案：D. eSpqp3-OwnF-9ari-aEKV-ljRq-KjcY-kLz5Ul

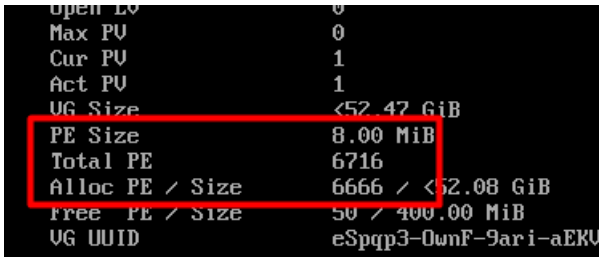
解答：



	15	**该卷组 Volume Group (VG)共有多少个LVM物理区域Physical E√tent (PE)?**
	A.	50
	B.	3210
	C.	3456
	D.	6666
√	E.	6716

答案：E. 6716

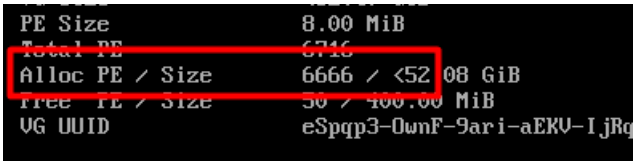
解答：



	16	该卷组Volume Group (VG)共划分了多少个物理区域Physical E√tent (PE)用了配置逻辑卷Logical Volume (LV)?
	A.	50
	B.	3210
	C.	3456
√	D.	6666
	E.	6716

答案：D. 6666

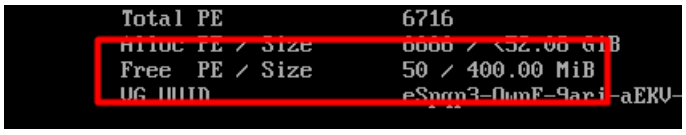
解答：



	17	该卷组Volume Group (VG)还余下多少个物理区域Physical E√tent (PE)未被配置使用？
√	A.	50
	B.	3210
	C.	3456
	D.	6666
	E.	6716

答案：A. 50

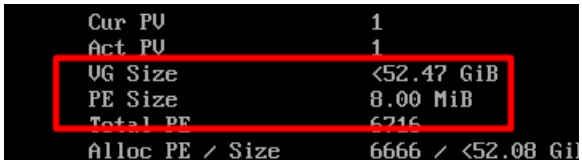
解答：



	18	就该卷组Volume Group (VG)而言，每个物理区域Physical E√tent (PE)的大小(size)是多少？
	A.	1 MB
	B.	2 MB
	C.	4 MB
√	D.	8 MB
	E.	16 MB

答案：D. 8 MB

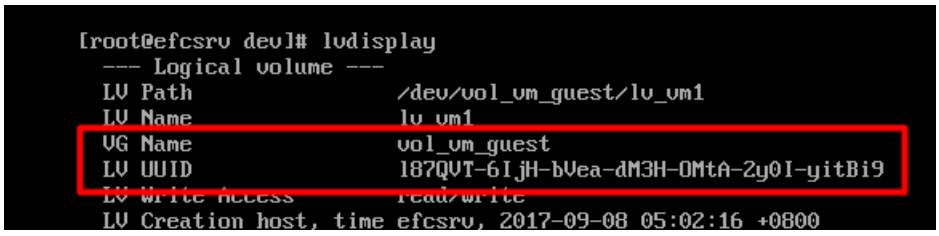
解答：



	19	事实上，该卷组Volume Group (VG) 共配置了两个逻辑卷组Logical Volume (LV)，第一个逻辑卷组Logical Volume (LV) UUID是 ？
√	A.	l87QVT-6IjH-bVea-dM3H-OMtA-2y0I-yitBi9
	B.	ysHo03-FFL9-0Tfl-zOeO-O7fn-TPz√-2p4mu0
	C.	UGpPyJ-ISUZ-eGJh-hrny-qPFY-UFUA-DfZ8mw
	D.	eSpqp3-OwnF-9ari-aEKV-IjRq-KjcY-kLz5Ul
	E.	UGpPyJ-ISUZ-eGJh-aEKV- OMtA-2y0I-yitBi9

答案：A. l87QVT-6IjH-bVea-dM3H-OMtA-2y0I-yitBi9

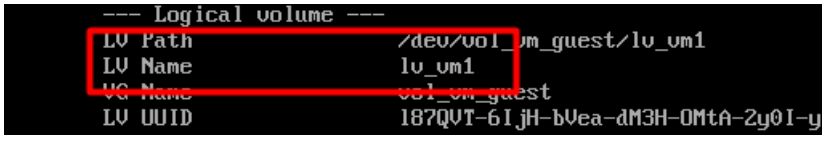
解答：



	20	上述第一个逻辑卷组Logical Volume (LV)的名称是什么 ？
	A.	/dev/loop0
	B.	vol_vm_guest
	C.	vol_guest
√	D.	lv_vm1
	E.	lv_vm2

答案：D. lv_vm1

解答：

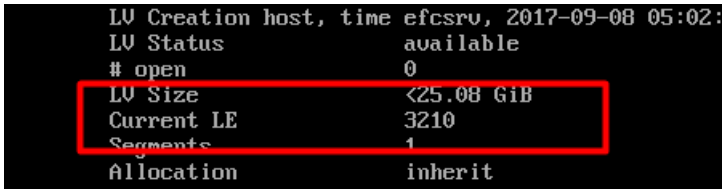


	21	上述第一个逻辑卷组Logical Volume (LV)共占据了多少物理区域Physical E√tent (PE) ？
	A.	50
√	B.	3210

	21	上述第一个逻辑卷组Logical Volume (LV)共占据了多少物理区域Physical E√tent (PE)？
	C.	3456
	D.	6666
	E.	6716

答案：B. 3210

解答：



	22	上述第一个逻辑卷组Logical Volume (LV)的建立时间是什么？
	A.	2017-09-06 05:02:16 +0800
	B.	2017-09-07 05:02:16 +0800
√	C.	2017-09-08 05:02:16 +0800
	D.	2017-09-09 05:02:16 +0800
	E.	2017-09-10 05:02:16 +0800

答案：C. 2017-09-08 05:02:16 +0800

解答：

	23	在上述第一个逻辑卷组Logical Volume (LV)当中，储存有一个名为duncan.mark的文件，下列哪项为其MD5哈希值(Hash value)?
	A.	01daa9fb8d1cc386bffb0c25ff57d7ea
√	B.	8da97369e625574d1d8145d49ca9b61c
	C.	b69894efe2f03d43d95d98856ea21674
	D.	74c5d7a6500d63a0308f2fc54a03eb0d
	E.	43309465540a069357182af1da438a07

答案：B. 8da97369e625574d1d8145d49ca9b61c

解答：

```
文件名: duncan.mark
文件扩展名: mark
逻辑大小(字节): 37
访问时间: 2017-10-31 10:09:25
创建时间: 2017-09-08 11:29:37
修改时间: 2017-09-08 11:30:01
描述: 文件
物理大小(字节): 4,096
物理位置: 141,557,760
物理扇区: 276,480
MD5值: 8DA97369E625574D1D8145D49CA9B61C
SHA-1值: BE8471762FB321B3645198B723F07711491540F9
SHA-256值: E85C8FD747A0BE581E7AF9255907F84C7571B9D8DCEBFC964AA31220318EBCA2
原始路径: lv_vm1 \分区1[hda0]:\duncan.mark
完整路径: 2017团队\lv_vm1 \分区1[hda0]:\duncan.mark
```

CSDN @A349 奇乃正

	24	在该卷组Volume Group (VG) 共配置了两个逻辑卷组Logical Volume (LV)，其中有一个逻辑卷组Logical Volume (LV)是用作运行Ubuntu 系统，该逻辑卷Logical Volume (LV) UUID是 什么？
	A.	l87QVT-6IjH-bVea-dM3H-OMtA-2y0l-yitBi9
	B.	ysHo03-FFL9-0Tfl-zOeO-O7fn-TPz√-2p4mu0
√	C.	UGpPyJ-lSUZ-eGJh-hrny-qPFY-UFUA-DfZ8mw
	D.	eSpqp3-OwnF-9ari-aEKV-ljRq-KjcY-kLz5Ul
	E.	UGpPyJ-lSUZ-eGJh-aEKV- OMtA-2y0l-yitBi9

答案：C. UGpPyJ-lSUZ-eGJh-hrny-qPFY-UFUA-DfZ8mw

解答：

```
LV Path                /dev/vol_vm_guest/lv_vm2
LV Name                lv_vm2
VG Name                vol_vm_guest
LV UUID                UGpPyJ-lSUZ-eGJh-hrny-qPFY-UFUA-DfZ8mw
LV Write Access        read/write
LV Creation host, time efcsrv, 2017-09-08 05:02:25 +0800
LV Status              available
# open                 0
LV Size                27.00 GiB
Current LE             3456
Segments               1
Allocation             inherit
Read ahead sectors     auto
- currently set to     4096
Block device           253:1
```

CSDN @A349 奇乃正

	25	在上述逻辑卷组Logical Volume (LV)当中，储存有一个名为lora.mark的文件，下列哪项为其MD5哈希值(Hash value)?
	A.	01daa9fb8d1cc386bffb0c25ff57d7ea
	B.	8da97369e625574d1d8145d49ca9b61c
	C.	b69894efe2f03d43d95d98856ea21674
√	D.	74c5d7a6500d63a0308f2fc54a03eb0d
	E.	43309465540a069357182af1da438a07

答案：D. 74c5d7a6500d63a0308f2fc54a03eb0d

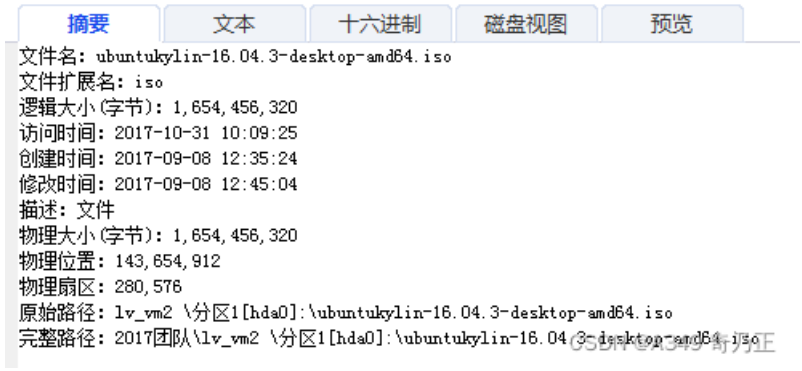
解答：

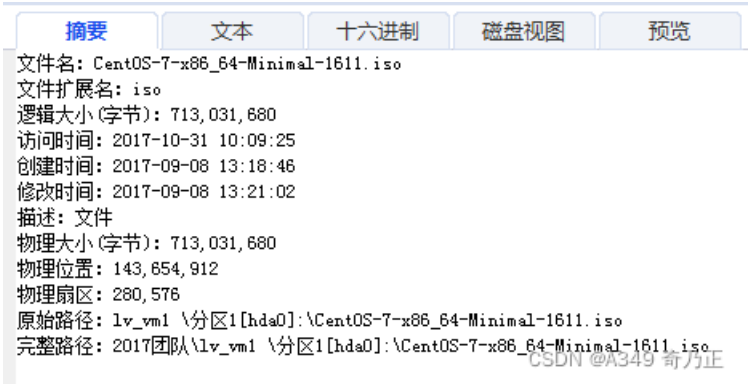
3 VM

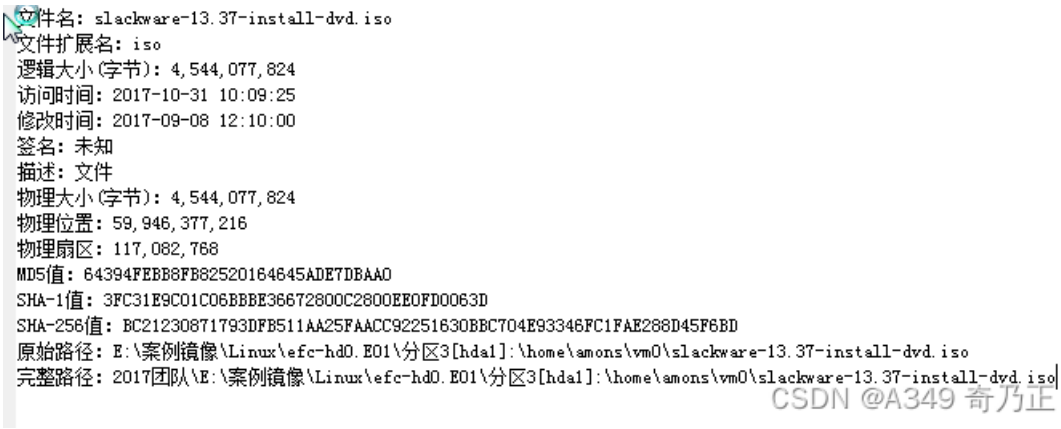
	26	事实上，上述被检取作法证检验的LINU√系统，曾经运行了三个虚拟机器(Virtual Machine, VM)，下列哪项组合包含了上述全部曾运行的虚拟机器？
	i	Gentoo
	ii	Slackware
	iii	Ubuntu
	iv	Antergos
	v	CentOS
	A.	(i), (ii) 及 (iii)
	B.	(i), (iii) 及 (iv)
	C.	(i), (iii) 及 (v)
√	D.	(ii), (iii) 及 (v)
	E.	(i), (iii) 及 (v)

答案：D. (ii), (iii) 及 (v)

解答：



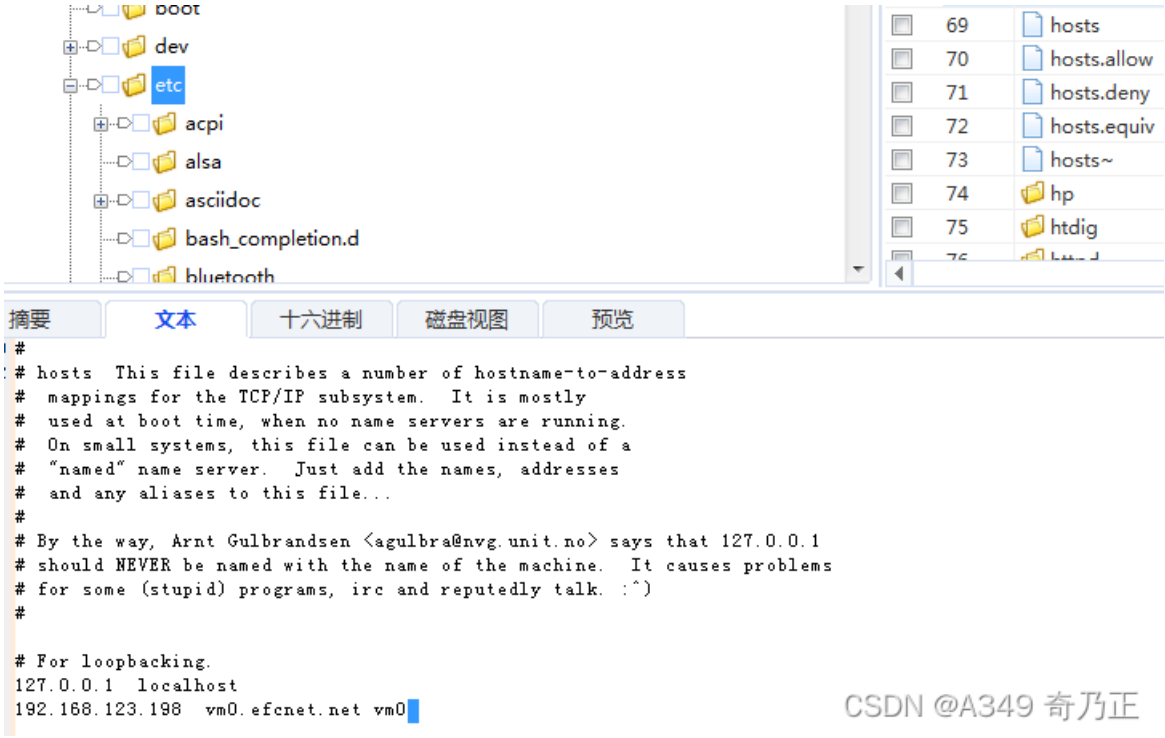




	27	在上述三个虚拟机器(Virtual Machine, VM)当中，其中有一个储存了可用作编程(Coding)的勒索软件源码(Source Code)，它是使用了下列哪个本地IP 地址 (Local IP Address) ?
√	A.	192.168.122.198
	B.	192.168.10.10
	C	192.168.122.214
	D.	192.168.122.157
	E.	192.168.122.2

答案：A. 192.168.122.198

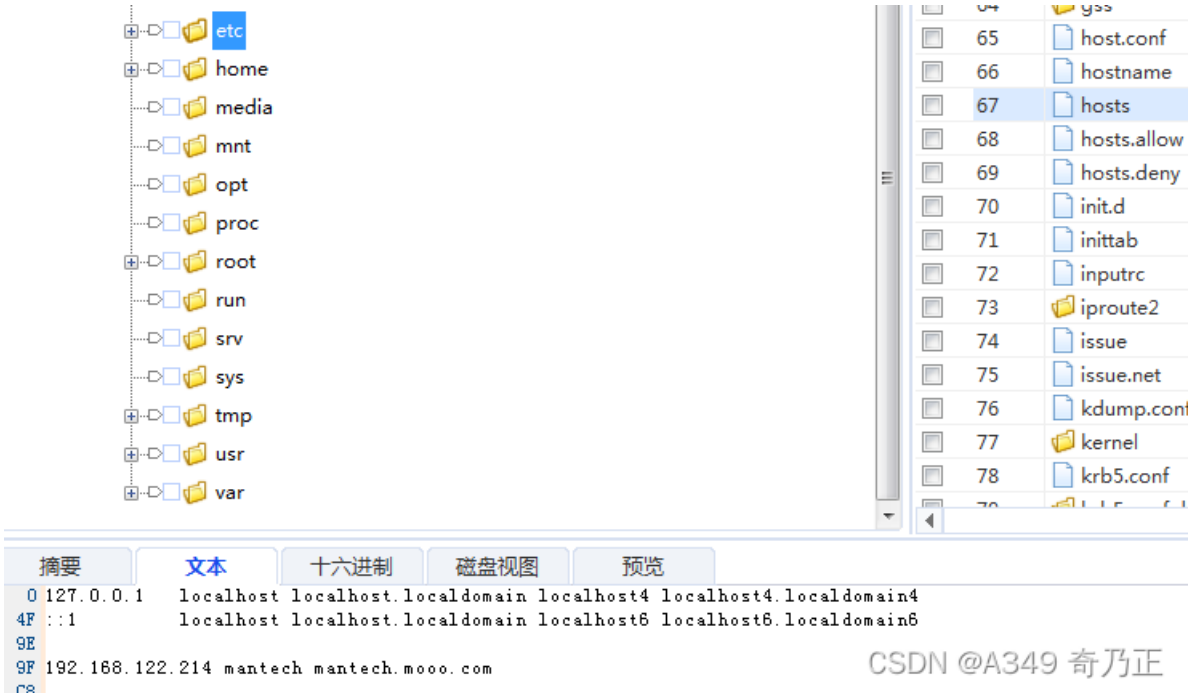
解答：



	28	**在上述三个虚拟机器(Virtual Machine, VM)当中，其中一个曾经安装并运行过私有云软件，它是使用下列哪个本地IP 地址(Local IP Address)？**
	A.	192.168.122.198
	B.	192.168.10.10
√	C	192.168.122.214
	D.	192.168.122.157
	E.	192.168.122.2

答案：C. 192.168.122.214

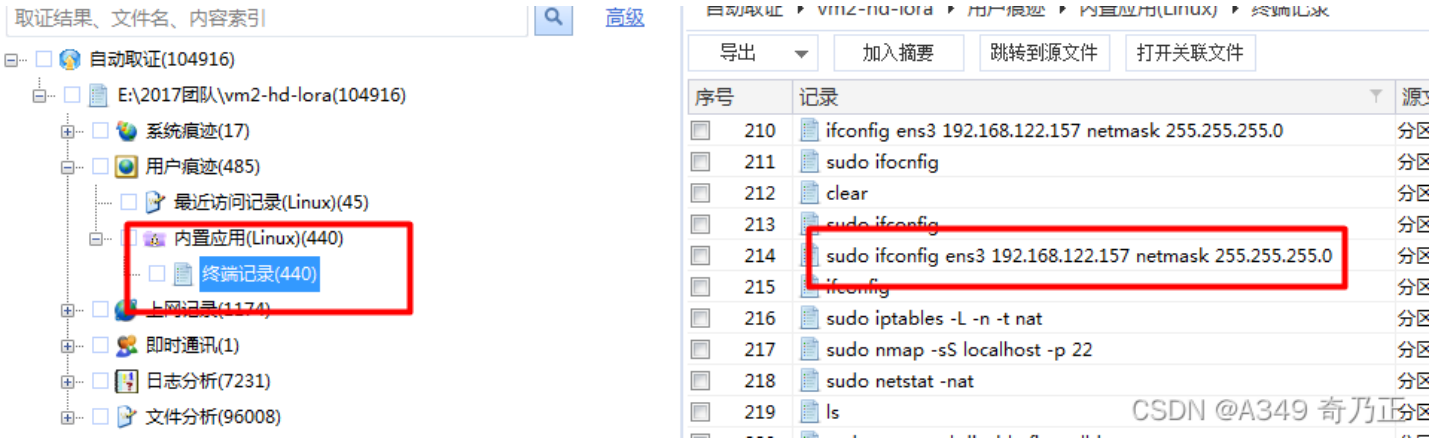
解答：



	29	在上述三个虚拟机器(Virtual Machine, VM)当中，其中一个安装了FTP服务器服务，它是使用下列哪个本地IP 地址 (Local IP Address)？
	A.	192.168.122.198
	B.	192.168.10.10
	C	192.168.122.214
√	D.	192.168.122.157
	E.	192.168.122.2

答案：D. 192.168.122.157

解答：

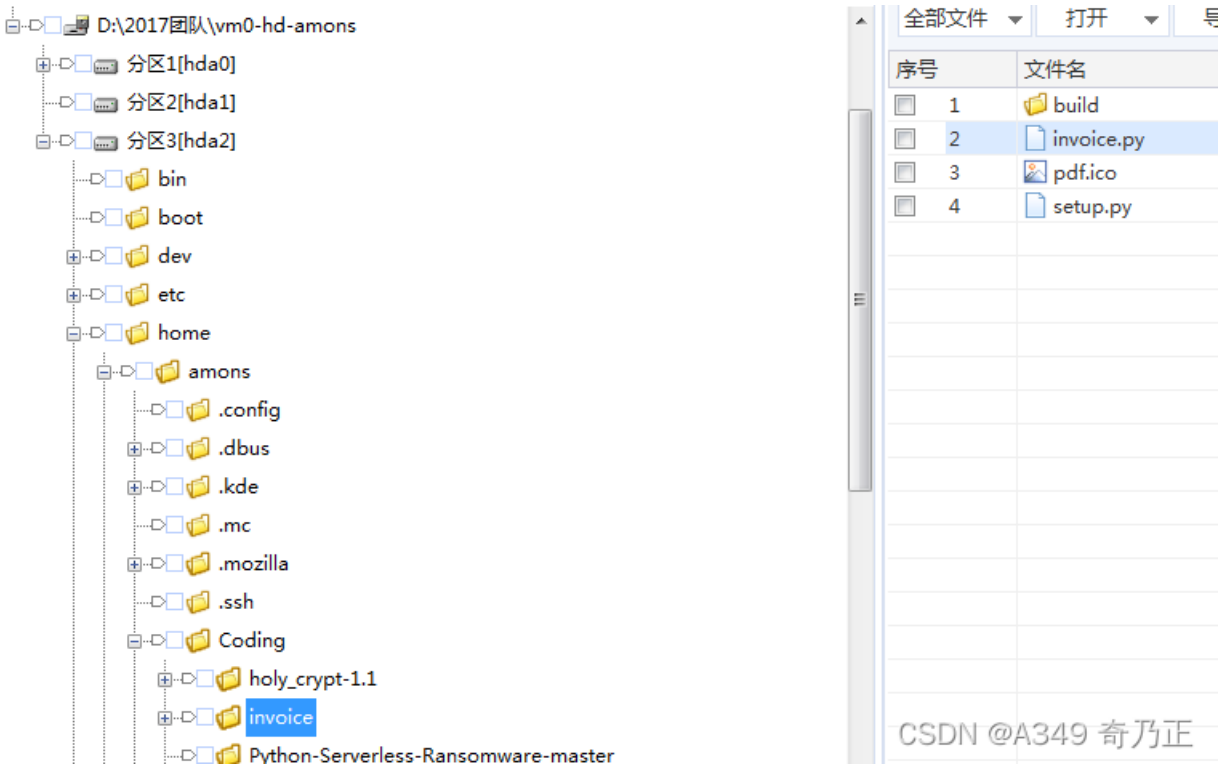


VM0

	30	在个人竞赛中，Gary的手提电脑(Win7 OS)发现有勒索程序invoice.e√e。就是次团体竞赛中，于题27中提及过的虚拟机器(Virtual Machine, VM)里，在哪个位置能发现此勒索程序的原始代码？
	A.	…/Python-Serverless-Ransomware-master/…
	B.	…/holy_crypt-1.1/…
	C	…/setuptools-master/…
√	D.	…/invoice/…
	E.	…/ransomware-master/…

答案：D. …/invoice/…

解答：



	31	根据上述勒索程序的原始代码，哪行程序代码显示该程序进行自我复制(Self-replication)?
	A.	8
	B.	70
√	C	74
	D.	84
	E.	119

答案：C.74

解答：

```
72  os.system('mkdir \\tmp > tmp111')
73  os.system(cmd)
74  os.system('REG ADD "HKCU\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run" /V "My App" /t REG_SZ /F /D "C:\\tmp\invoice.exe > tmp111')
75  os.system('del tmp111')
76  os.system('bcdedit /set {default} recoveryenabled No')
77  os.system('bcdedit /set {default} bootstatuspolicy ignoreallfailures')
```

	32	根据上述勒索程序的原始代码，哪行程序代码显示开始进行文件加密(Encryption)?
√	A.	8
	B.	70
	C	74
	D.	84
	E.	119

答案：A. 8

解答：

```
5
6
7
8  def encrypt(key, FileName):
9      chunkS = 64 * 1024
10     OutputFile = os.path.join(os.path
11     Fsize = str(os.path.getsize(FileN
12     IniVect = ''
```

	33	根据上述勒索程序的原始代码，该程序总共能加密多少类型文件？
	A.	19
√	B.	20
	C	21
	D.	22
	E.	不能加密

答案：B.20

解答：

```
valid_extension = [".txt", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".odt", ".jpg", ".png", ".csv", ".sql", ".mdb", ".sln", ".php", ".asp", ".aspx", ".html", ".xml", ".psd"]
```

	34	根据上述勒索程序的原始代码，该程序是使用何种加密标准？
	A.	Data Encryption Standard (DES)
√	B.	Advanced Encryption Standard (AES)
	C	RSA (Rivest–Shamir–Adleman)
	D.	Twofish
	E.	Blowfish

答案：B. Advanced Encryption Standard (AES)

解答：

```
1  from Crypto.Hash import SHA256
2  from Crypto.Cipher import AES
3  import os, random, sys
4  import webbrowser
5
```

	35	根据上述勒索程序的原始代码，哪行程序代码显示连接指挥及控制(Command & Control, C&C)服务器。
	A.	2
	B.	70
	C	74
	D.	84
√	E.	119

答案：E.119

解答：

```
117
118
119        webbrowser.open('http://223.17.250.208:6060/C&C/')
120
121
```

VM1

	36	于题28中提及过的虚拟机器(Virtual Machine, VM)曾经运行过一个私有云软件，提供私有云服务，并储存有一个于2017年 10月30日建立的PCAP文件，下列哪个是其MD5哈希值(Hash value)?
√	A.	36a179aebadcd697e11bf0bbad7c4d8a
	B.	88ac535e35792b72efd768c2f8c11f94
	C	9e4bf671e1d44da9e085c4c790116e59
	D.	0ac9f639679361708832c77950f93be2
	E.	1b385451a788a825673c31862566e0a5

答案：A. 36a179aebadcd697e11bf0bbad7c4d8a

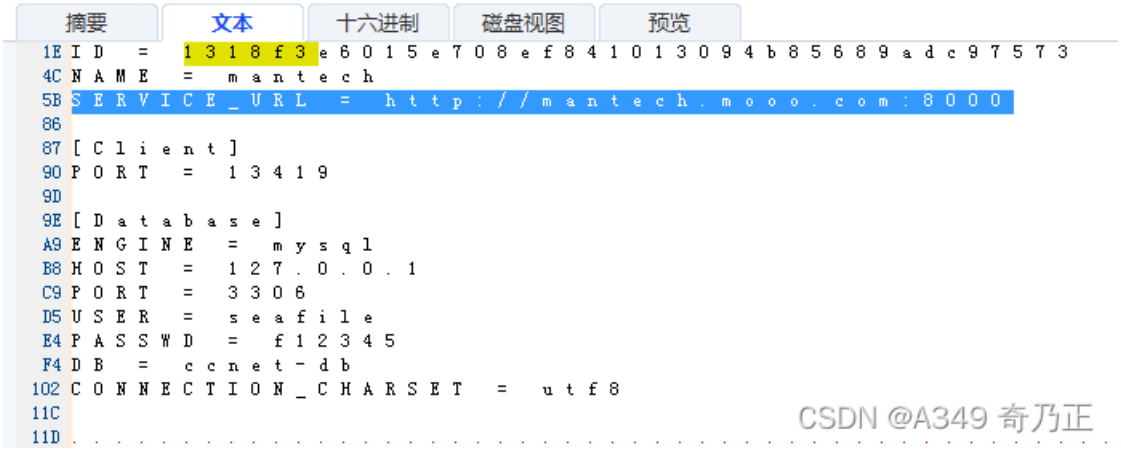
解答：

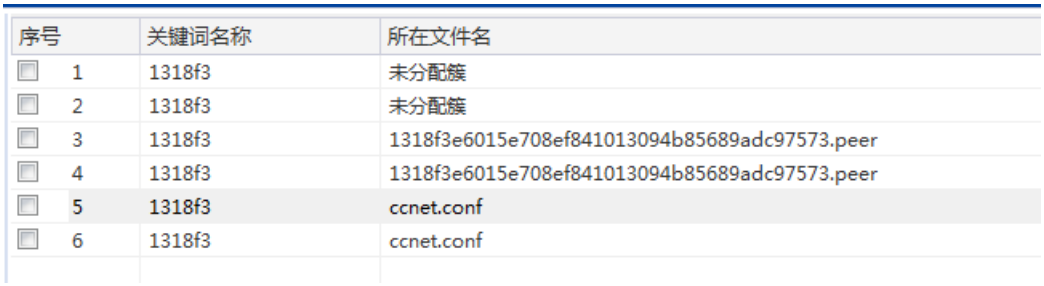
	37	运行在此虚拟机器(Virtual Machine, VM)的私有云软件，根据其设定，下列哪项是其对外连结的URL?
	A.	http://mantech.mood.com:8000
√	B.	http://mantech.mooo.com:8000
	C	http://mantech.mooo.com:8080

	37	运行在此虚拟机器(Virtual Machine, VM)的私有云软件，根据其设定，下列哪项是其对外连结的URL?
	D.	http://mantech.mooo.com:8088
	E.	http://mantech.mooe.com:8000

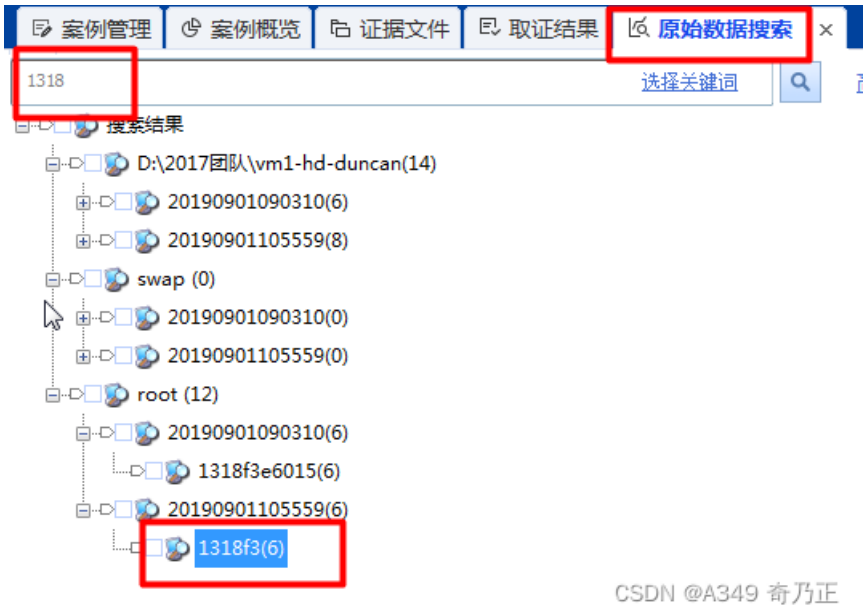
答案：B. http://mantech.mooo.com:8000

解答:





序号	关键词名称	所在文件名
1	1318f3	未分配簇
2	1318f3	未分配簇
3	1318f3	1318f3e6015e708ef841013094b85689adc97573.peer
4	1318f3	1318f3e6015e708ef841013094b85689adc97573.peer
5	1318f3	ccnet.conf
6	1318f3	ccnet.conf

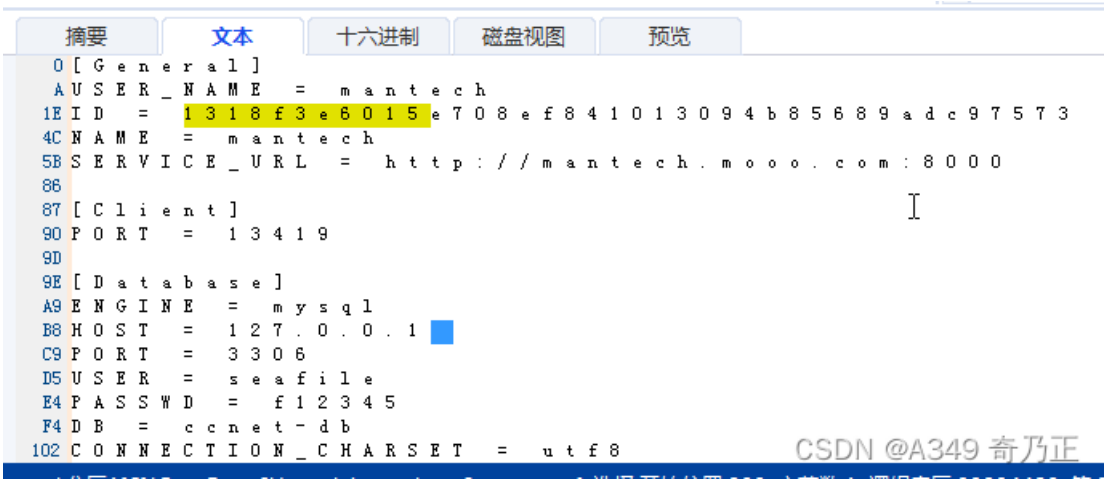


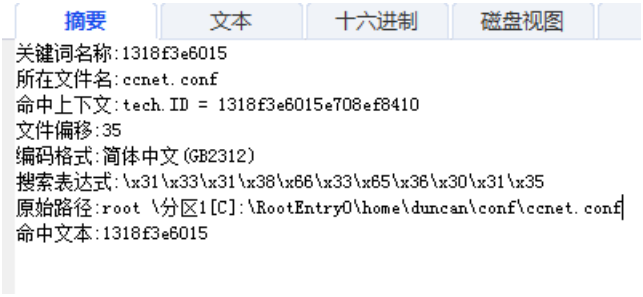
	38	此私有云软件，会使用内置RPC框架(Internal RPC framework)，其ID是什么？[注: RPC – 远端过程调用 (Remote Procedure Call)]
	A.	f3e6015c708ef841013094b83689adc97573
	B.	1318f3e6015d708ef841013094b84689adc97573

	38	此私有云软件，会使用内置RPC框架(Internal RPC framework)，其ID是什么？[注: RPC – 远端过程调用 (Remote Procedure Call)]
√	C	1318f3e6015e708ef841013094b85689adc97573
	D.	1318f3e6015f708ef841013094b95689adc97573
	E.	1318f3e6015g708ef841013094b05689adc97573

答案：C. 1318f3e6015e708ef841013094b85689adc97573

解答：

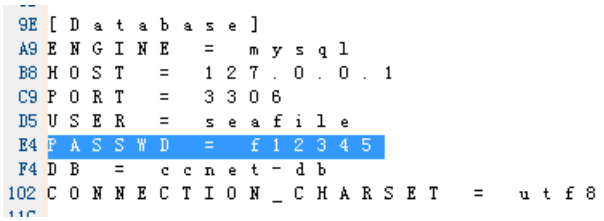


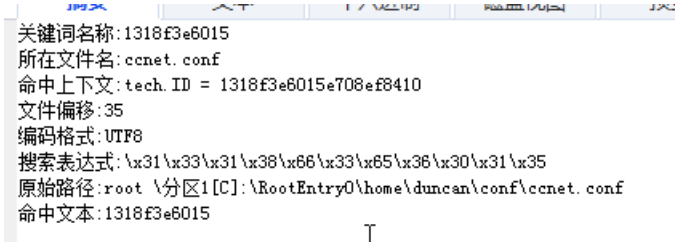


	39	此虚拟机器(Virtual Machine, VM)中的私有云软件，会连接上一个本地MySQL 数据库，登入密码是什么？
	A.	f0123
√	B.	f1234
	C	f1334
	D.	f1134
	E.	f2345

答案：B. f12345

解答：

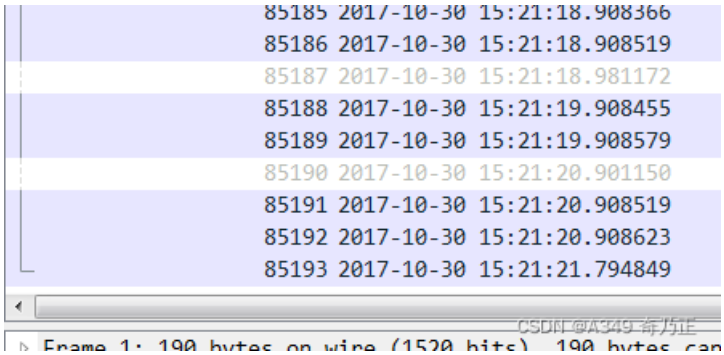




	40	在上述运行私有云软件的虚拟机器(Virtual Machine, VM)中，遗留了一个以日期为文件名称的PCAP文件，它共记录了多少个数据包(Packet)?
√	A.	85193
	B.	85194
	C.	85195
	D.	85196
	E.	85197

答案：A. 85193

解答：

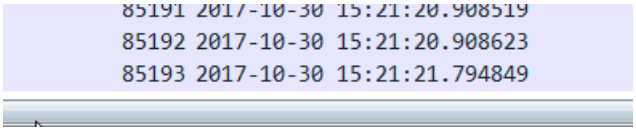


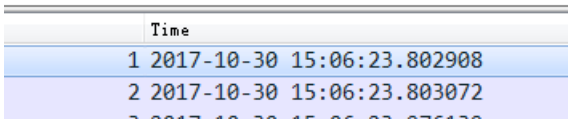
	41	上述PCAP文件共占据了多少时间?
	A.	14分47秒
√	B.	14分57秒
	C.	15分37秒

	41	上述PCAP文件共占据了多少时间？
	D.	15分47秒
	E.	15分57秒

答案：B.14分57秒

解答：

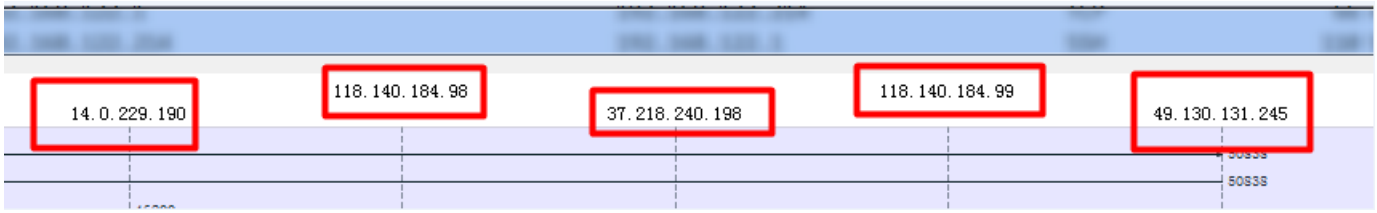


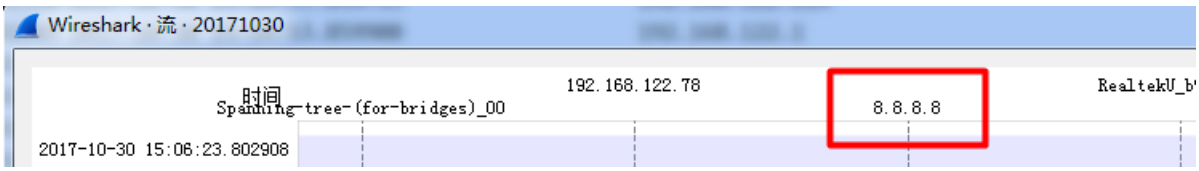


	42	上述PCAP文件记录了多少个公共IP地址(Public IP)？
	A.	3
	B.	4
	C.	5
√	D.	6
	E.	7

答案：D.6

解答：

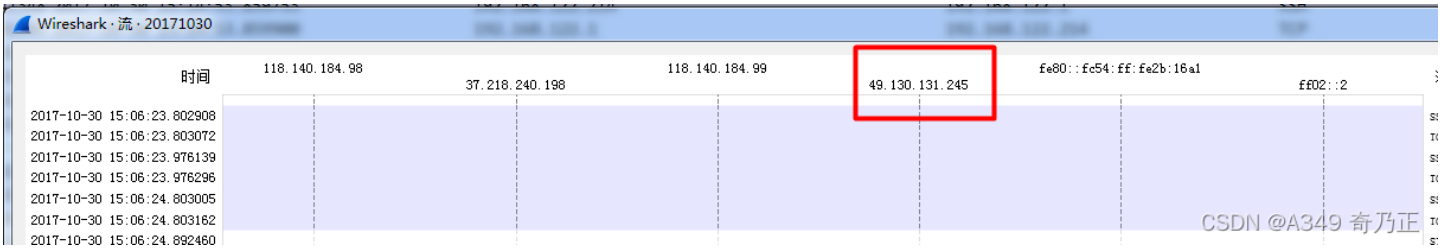




	43	根据上述PCAP文件，总流量值最高的公共IP地址是哪个？
	A.	14.0.229.190
√	B.	49.130.131.245
	C.	118.140.184.98
	D.	37.218.240.198
	E.	37.218.240.199

答案：B.49.130.131.245

解答：



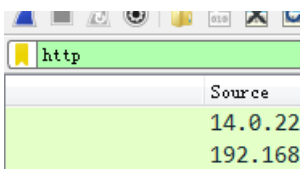
	44	根据上述PCAP文件，最高下载流量的公共IP地址是哪个？
√	A.	14.0.229.190
	B.	49.130.131.245
	C.	118.140.184.98
	D.	37.218.240.198
	E.	37.218.240.199

答案：A. 14.0.229.190

解答：

14.0.229.190	192.168.122.214	HTTP	503 GET /thumbnail/302b7384
192.168.122.214	14.0.229.190	HTTP	59 HTTP/1.1 200 OK (PNG)
14.0.229.190	192.168.122.214	HTTP	503 GET /thumbnail/302b7384
192.168.122.214	14.0.229.190	HTTP	59 HTTP/1.1 200 OK (PNG)
14.0.229.190	192.168.122.214	HTTP	503 GET /thumbnail/302b7384
192.168.122.214	14.0.229.190	HTTP	59 HTTP/1.1 200 OK (PNG)
14.0.229.190	192.168.122.214	HTTP	622 GET /thumbnail/302b7384
192.168.122.214	14.0.229.190	HTTP	59 HTTP/1.1 200 OK (appli
14.0.229.190	192.168.122.214	HTTP	503 GET /thumbnail/302b7384
192.168.122.214	14.0.229.190	HTTP	59 HTTP/1.1 200 OK (PNG)
14.0.229.190	192.168.122.214	HTTP	503 GET /thumbnail/302b7384
192.168.122.214	14.0.229.190	HTTP	59 HTTP/1.1 200 OK (PNG)
14.0.229.190	192.168.122.214	HTTP	503 GET /thumbnail/302b7384
192.168.122.214	14.0.229.190	HTTP	59 HTTP/1.1 200 OK (PNG)
14.0.229.190	192.168.122.214	HTTP	503 GET /thumbnail/302b7384
14.0.229.190	192.168.122.214	HTTP	503 GET /thumbnail/302b7384
192.168.122.214	14.0.229.190	HTTP	59 HTTP/1.1 200 OK (PNG)
192.168.122.214	14.0.229.190	HTTP	59 HTTP/1.1 200 OK (PNG)
14.0.229.190	192.168.122.214	HTTP	622 [TCP Spurious Retransmi
14.0.229.190	192.168.122.214	HTTP	455 GET /media/img/file/24/
192.168.122.214	14.0.229.190	HTTP	919 HTTP/1.1 200 OK (PNG)
14.0.229.190	192.168.122.214	HTTP	503 [TCP Spurious Retransmi
14.0.229.190	192.168.122.214	HTTP	622 GET /thumbnail/302b7384
14.0.229.190	192.168.122.214	HTTP	508 GET /thumbnail/302b7384
192.168.122.214	14.0.229.190	HTTP	59 HTTP/1.1 200 OK (PNG)
192.168.122.214	14.0.229.190	HTTP	59 HTTP/1.1 200 OK (appli
14.0.229.190	192.168.122.214	HTTP	508 GET /thumbnail/302b7384
14.0.229.190	192.168.122.214	HTTP	622 GET /thumbnail/302b7384
192.168.122.214	14.0.229.190	HTTP	59 HTTP/1.1 200 OK (PNG)
192.168.122.214	14.0.229.190	HTTP	59 HTTP/1.1 200 OK (appli
14.0.229.190	192.168.122.214	HTTP	501 GET /media/img/grippy_l
192.168.122.214	14.0.229.190	HTTP	145 HTTP/1.1 200 OK (PNG)
14.0.229.190	192.168.122.214	HTTP	508 GET /thumbnail/302b7384

CSDN @A349 奇乃正

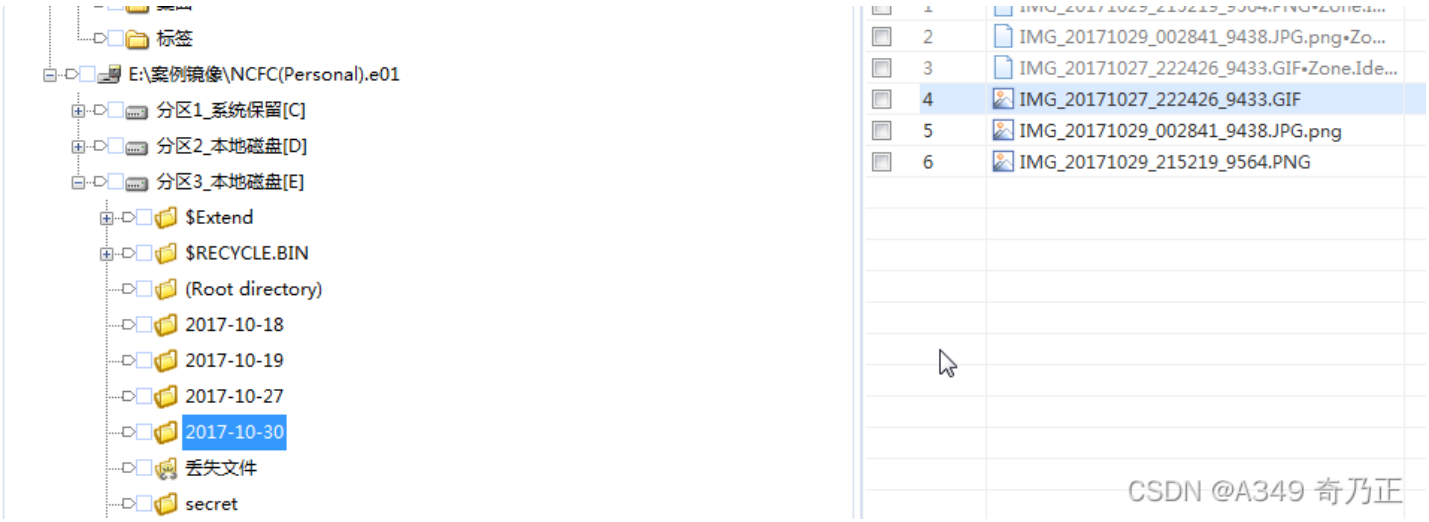


	45	根据调查得知，上述PCAP文件是前文提及的私有云软件尚在运作时的上传/下载资料记录。当中记录了Gary曾于该私有云浏览与案有关的枪械照片，共有三张(不计缩略图)。请按时间顺序，找出其MD5哈希值。 第一张枪械照片的MD5哈希值是什么？
	A.	89c68c45a7e4d10f409cf2764fd44c33

	45	根据调查得知，上述PCAP文件是前文提及的私有云软件尚在运作时的上传/下载资料记录。当中记录了Gary曾于该私有云浏览与案有关的枪械照片，共有三张(不计缩略图)。请按时间顺序，找出其MD5哈希值。 第一张枪械照片的MD5哈希值是什么？
	B.	d291d1da748ce7fb4ba408a6bbbcb222
√	C.	37088010ef0f8730c0f8600653b1fca2
	D.	9fd7afbdb5d682525509b3b57f4c0c91
	E.	003bc4bfbd364bd447648ea36cd1c514

答案：C. 37088010ef0f8730c0f8600653b1fca2

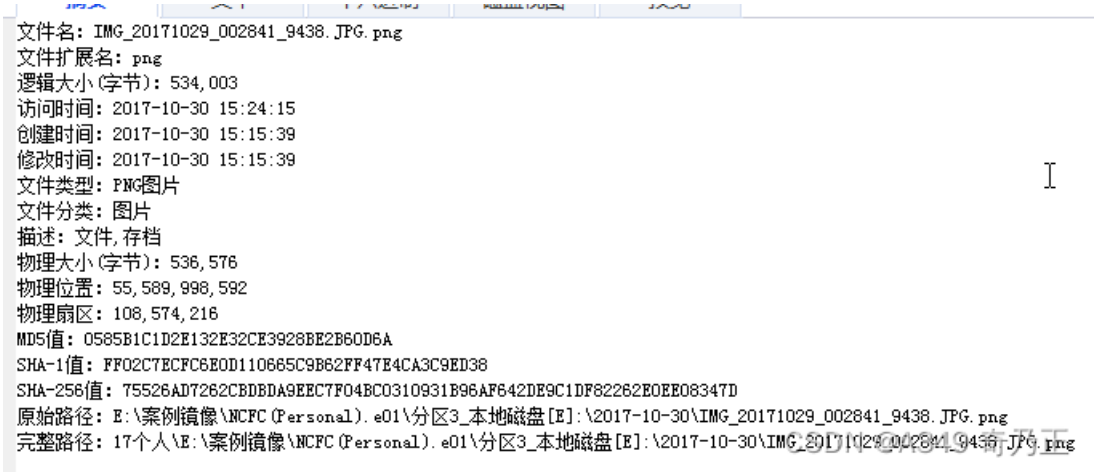
解答：



	46	第二张枪械照片的MD5哈希值是什么？
√	A.	0585b1c1d2e132e32ce3928be2b60d6a
	B.	e9a21071a5df65d43ea2a75fab51279e
	C.	5a078264ecd55918308a3164eefee7f3
	D.	a9c2962d2e0f31b067ae1b1d04ec9d94
	E.	b9b039a8aed7132cc9630788f9d698f2

答案：A. 0585b1c1d2e132e32ce3928be2b60d6a

解答：



	47	第三张枪械照片的MD5哈希值是什么？
	A.	b23d4610b0012ac47cb0f60bae8ee0a7
	B.	7c1bf67df7aab0db10c68f9646e9a674
	C.	bdbb0f0915790aa718d6837025ecf269
√	D.	f94398336683d9878f9ea7598f2e40dd
	E.	e533c315c7000ad15227a2670f606334

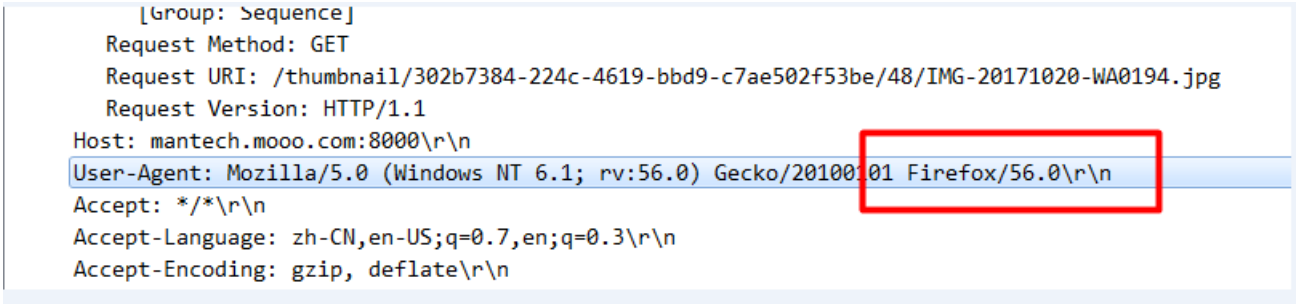
答案：D. f94398336683d9878f9ea7598f2e40dd

解答：

	48	上述枪械照片是经下列哪个浏览器软件浏览的？
	A.	Chrome
	B.	QQ Browser
	C.	Internet Explorer
√	D.	Firefox
	E.	Opera

答案：D. Firefox

解答：

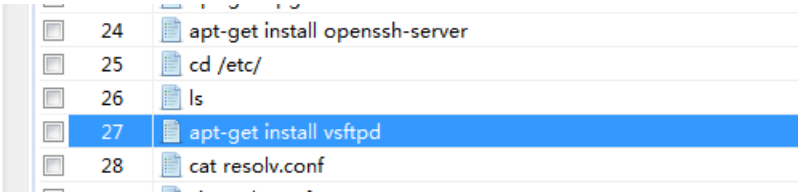


VM2

	49	在题29中提及过的虚拟机器(Virtual Machine, VM)，曾安装并提供过FTP服务，请问是下列哪种FTP?
√	A.	vsftp
	B.	gftp
	C	WinScp
	D.	ProFTP
	E.	Fire-FTP

答案：A. vsftp

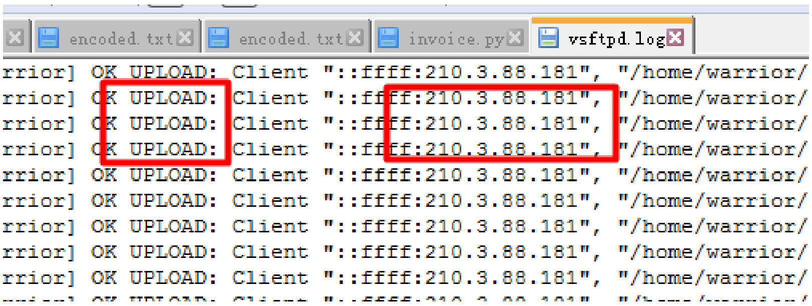
解答：

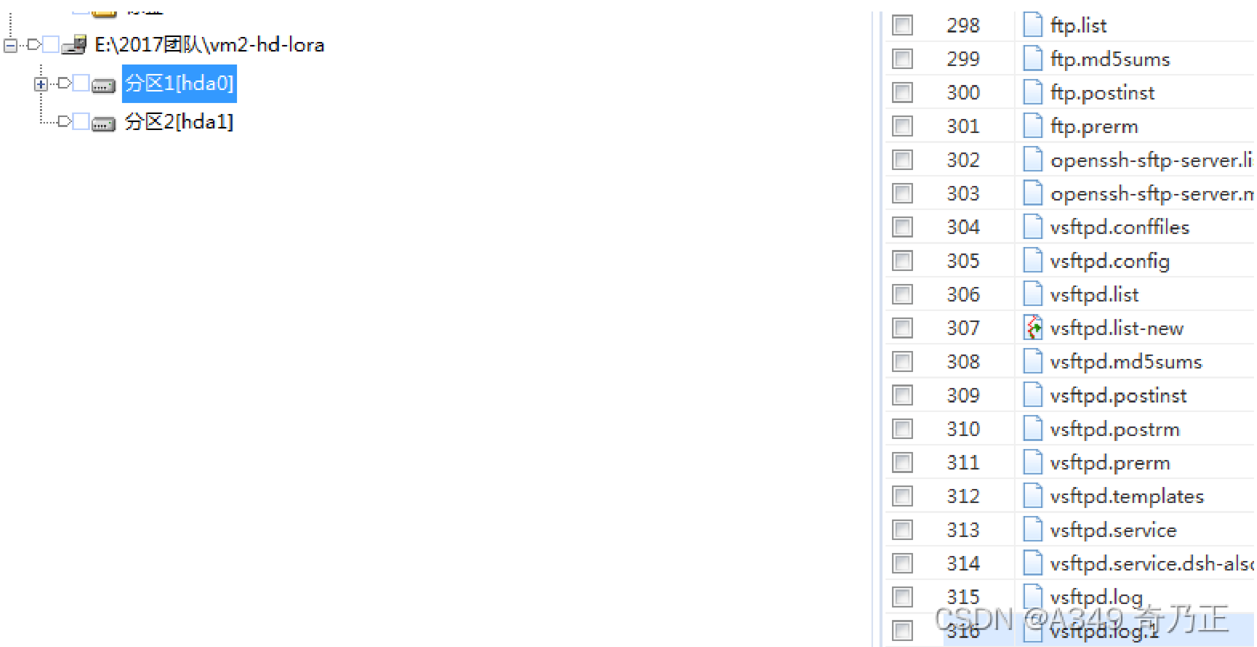


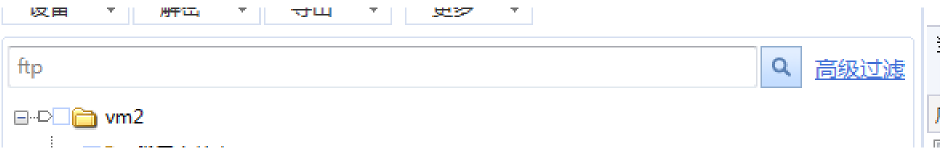
	50	根据该FTP服务器的日志，只记录了一个公共地址IP曾上传(UPLOAP)过资料，是下列哪个？
	A.	125.203.195.185
	B.	14.0.226.51
	C.	192.168.1.57
√	D.	210.3.88.181
	E.	45.64.240.68

答案：D. 210.3.88.181

解答：



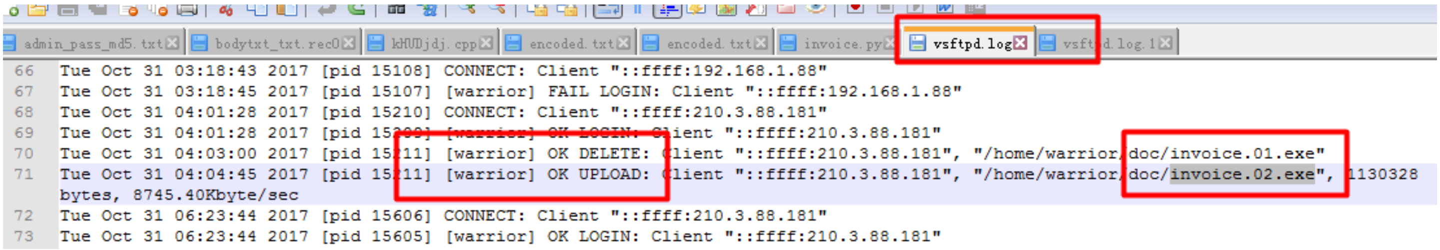


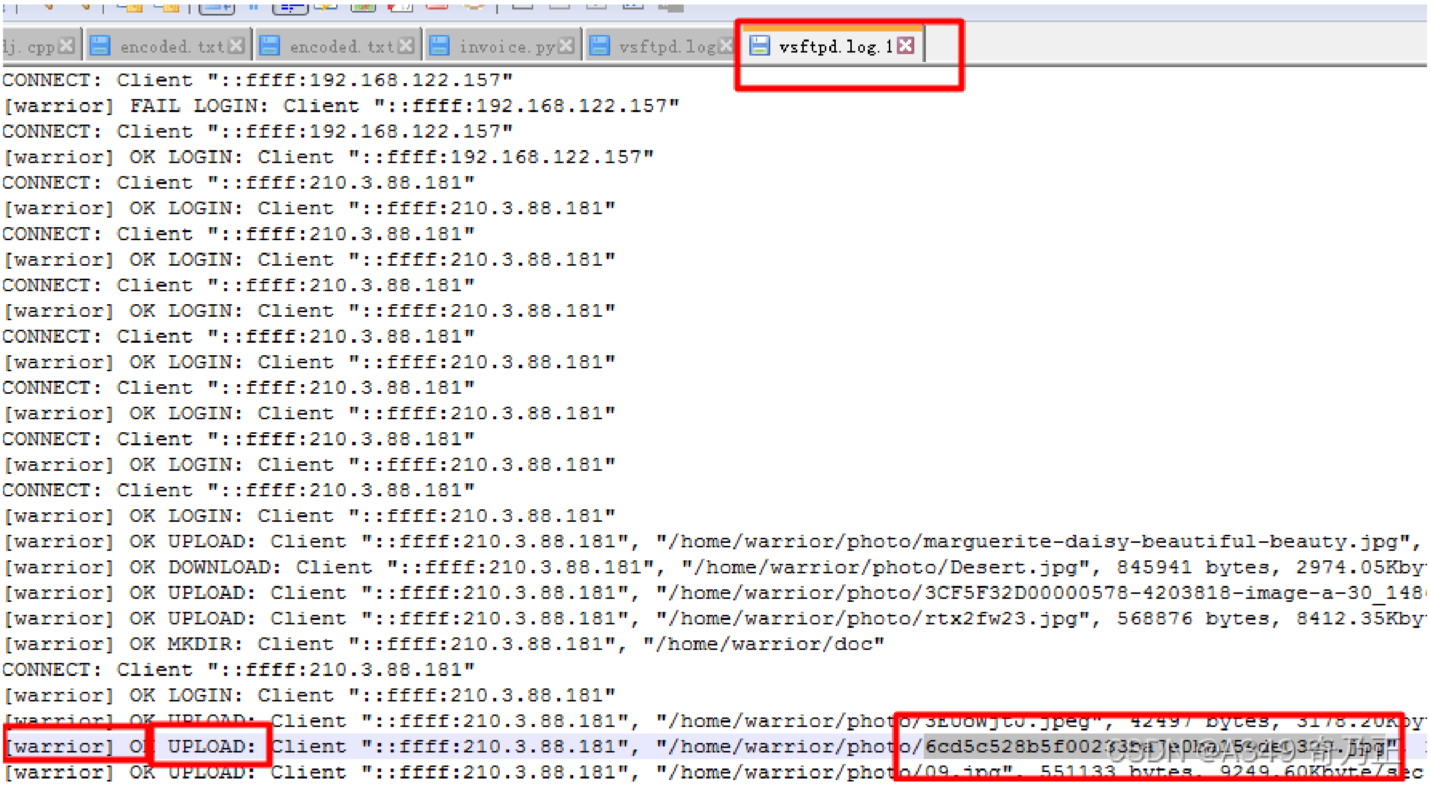


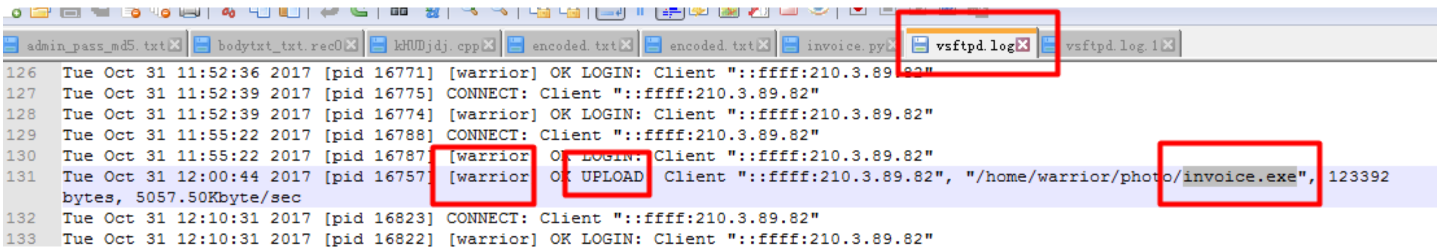
	51	根据该FTP服务器的日志，用户warrior曾上传过哪些资料？ Desert.jpg 6cd5c528b5f00233ba7e0ba154de0309.jpg Koala.jpg invoice.e√e invoice.02.e√e
	A.	i
	B.	i, ii
	C.	i, ii, iv
√	D.	ii,iv, v
	E.	i, iii, iv, v

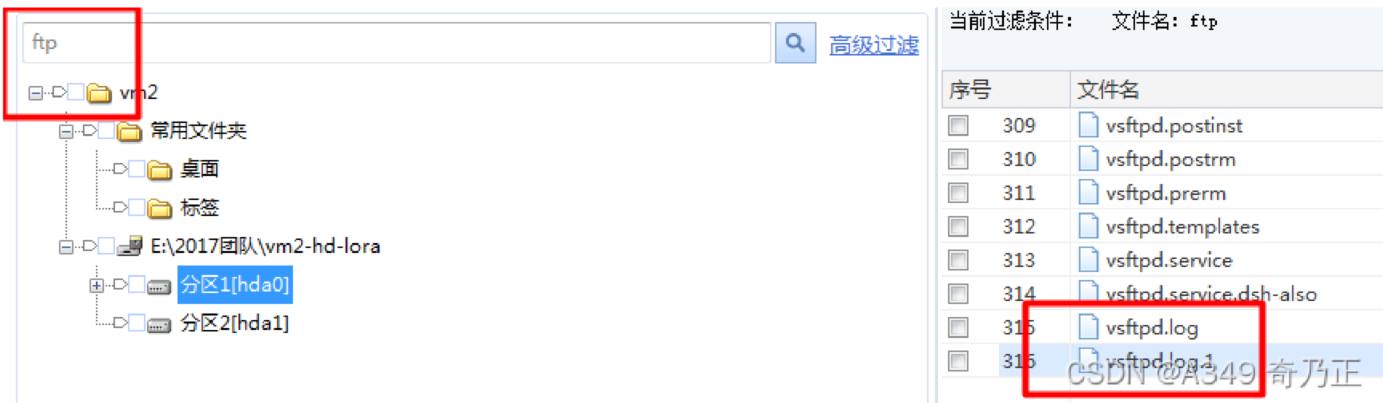
答案：D. ii,iv, v

解答：







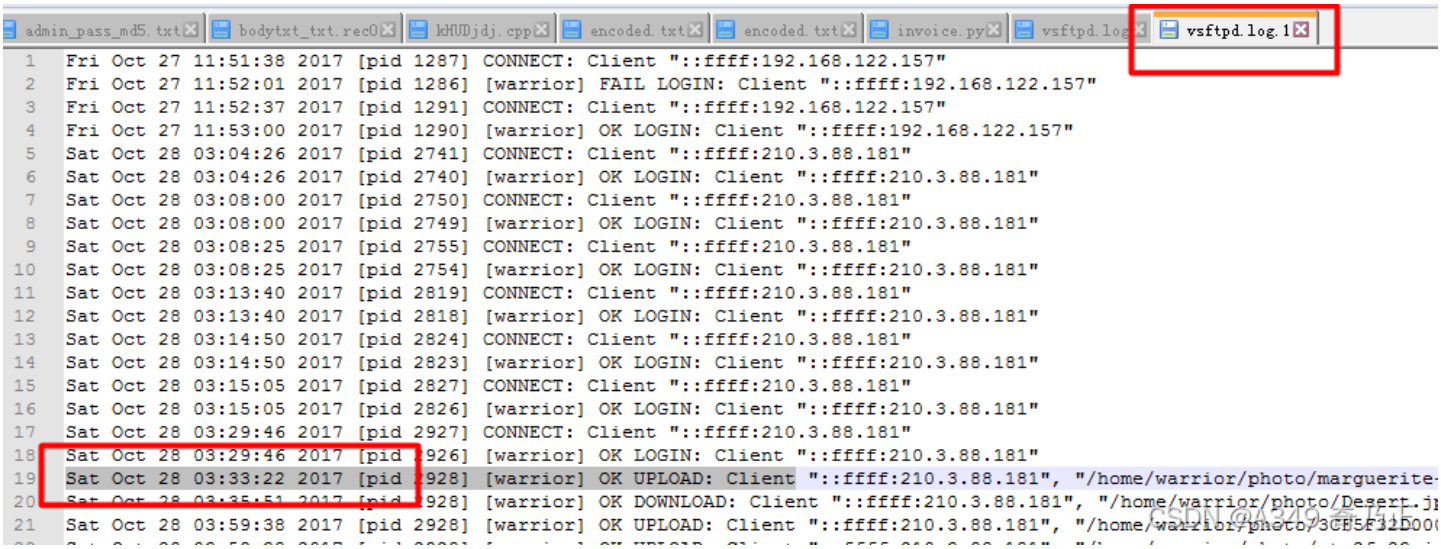


	52	根据该FTP服务器的日志，用户warrior第一次上传的时间为:
	A.	2017-10-27 11:51:38 (UTC)
	B.	2017-10-28 03:35:51 (UTC)
	C.	2017-10-28 09:44:28 (UTC)

	52	根据该FTP服务器的日志，用户warrior第一次上传的时间为:
√	D.	2017-10-28 03:33:22 (UTC)
	E.	2017-10-3102:01:30 (UTC)

答案：D. 2017-10-28 03:33:22 (UTC)

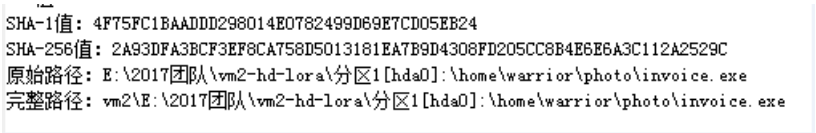
解答：



	53	上述安装了FTP 服务器服务的虚拟机器(Virtual Machine, VM)内，储存有一个名为invoice.e√e的执行文件，下列哪项是其储存位置？
	A.	/home/lora
	B.	/home/warrior/doc
√	C	/home/warrior/photo
	D.	/etc/doc-base
	E.	/var/log

答案：C. /home/warrior/photo

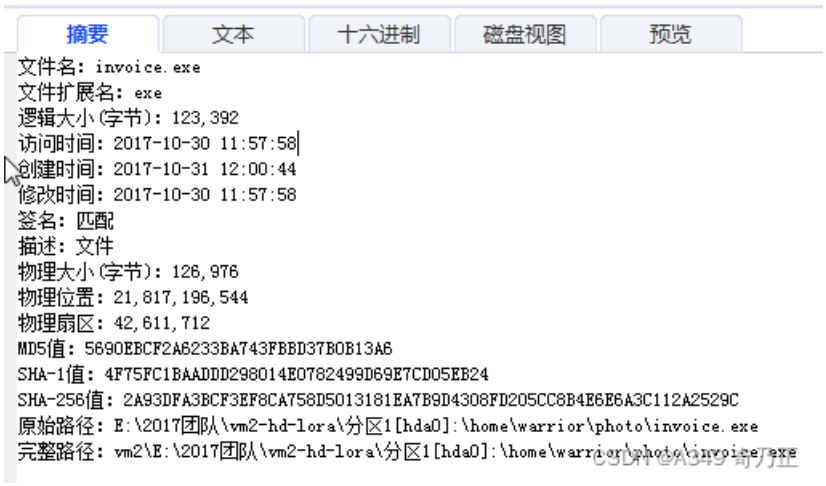
解答：



	54	上述执行文件invoice.e√e的MD5哈希值(Hash value)是什么？
	A.	9d377b10ce778c4938b3c7e2c63a229a
	B.	bdf3bf1da3405725be763540d6601144
√	C	5690ebcf2a6233ba743fbbd37b0b13a6
	D.	5a44c7ba5bbe4ec867233d67e4806848
	E.	fafa5efeaf3cbe3b23b2748d13e629a1

答案：C. 5690ebcf2a6233ba743fbbd37b0b13a6

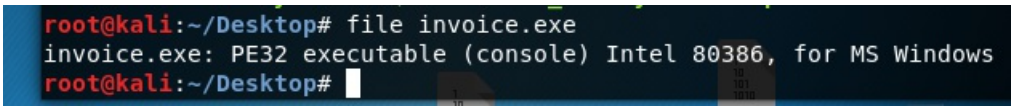
解答：



	55	**上述执行文件invoice.e√e是使用了什么执行文件格式(E√ecutable File Format)?**
√	A.	PE32
	B.	PE64
	C	ELF
	D.	COFF
	E.	XCOFF

答案：A. PE32

解答：

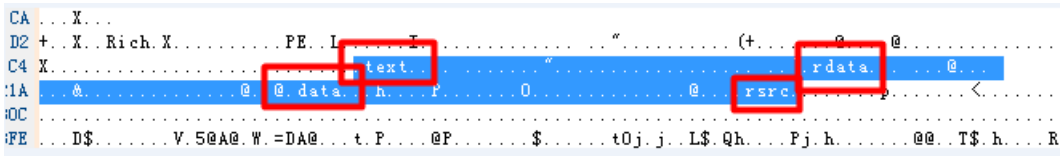


	56	**下列哪项不是上述执行文件invoice.exe的执行文件格式的节表(Section Table)?**
	A.	.text
	B.	.rdata
√	C	.reloc
	D.	.data

	56	下列哪项不是上述执行文件invoice.exe的执行文件格式的节表(Section Table)?
	E.	.rsrc

答案：C. .reloc

解答：这样查不是很准确，可以再用PEID查一下，这里忘记了截图。



Win8

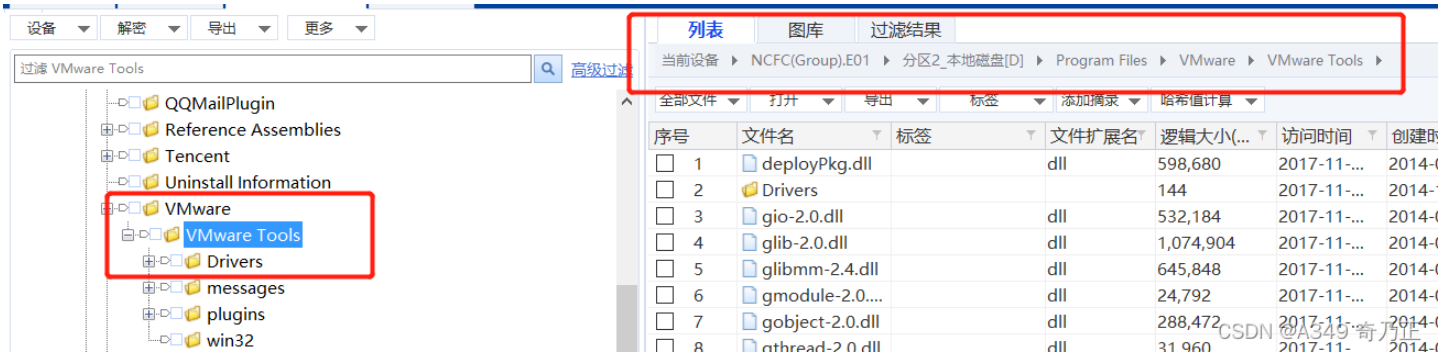
	57	Eric的手提电脑内的虚拟机器已成功取证并制作成法证镜像文件 (Forensic Image)，下列哪个是其MD5哈希值。
	A.	0CFB3A0BB016165F1BDEB87EE9F710C9
√	B.	F4089F7DA826DF56654C7AAE32D583C2
	C.	A0BB016160CFB3A0BB0161661670CFB3
	D.	16160CFB3A0BB016166A0BB016166167
	E.	FB3A0BB016165 B016166 A0DF7FJE2EJ0

解析：使用取证大师进行计算

	58	根据上述法证镜像文件 (Forensic Image)的显示，Eric是使用的下列哪个虚拟机？
	A.	Parallel
	B.	Virtual Box
√	C.	VMware

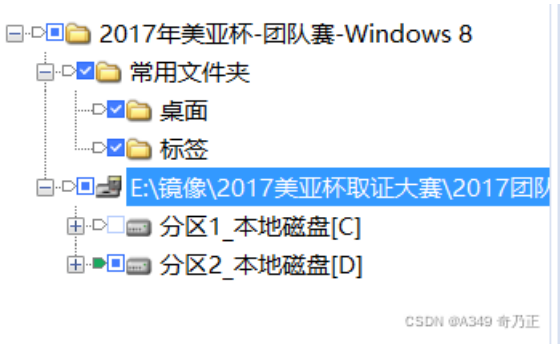
	58	根据上述法证镜像文件 (Forensic Image)的显示，Eric是使用的下列哪个虚拟机？
	D.	KVM
	E.	Xen

解析：在C盘下存在Program Files\Vmware文件夹，可确定使用的事VM虚拟机。



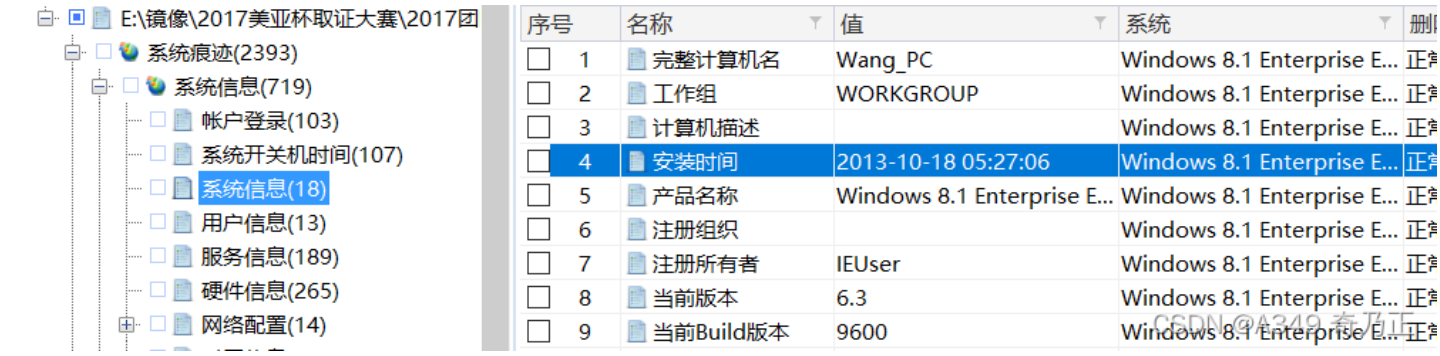
	59	根据法证镜像文件(Forensic Image)，内有多少个硬盘分区？
	A.	1
√	B.	2
	C.	3
	D.	4
	E.	5

解析：使用取证大师直接得出。



	60	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.	2013-10-17 21:27 UTC
	B.	2013-11-14 02:11 UTC
	C.	2017-09-28 06:16 UTC
	D.	2017-10-02 02:10 UTC
	E.	2017-10-03 12:14 UTC

解析：使用取证大师直接得出。

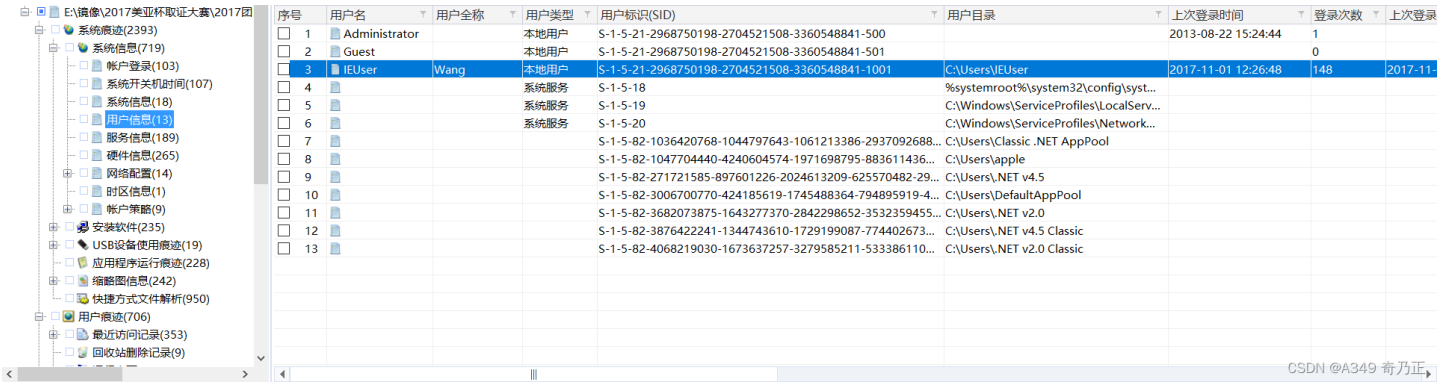


	61	用户“IEUSER " 的SID是什么？
	A.	500
	B.	1000
√	C.	1001
	D.	1005
	E.	1007

解析：取证大师-系统痕迹-系统信息-用户信息可得

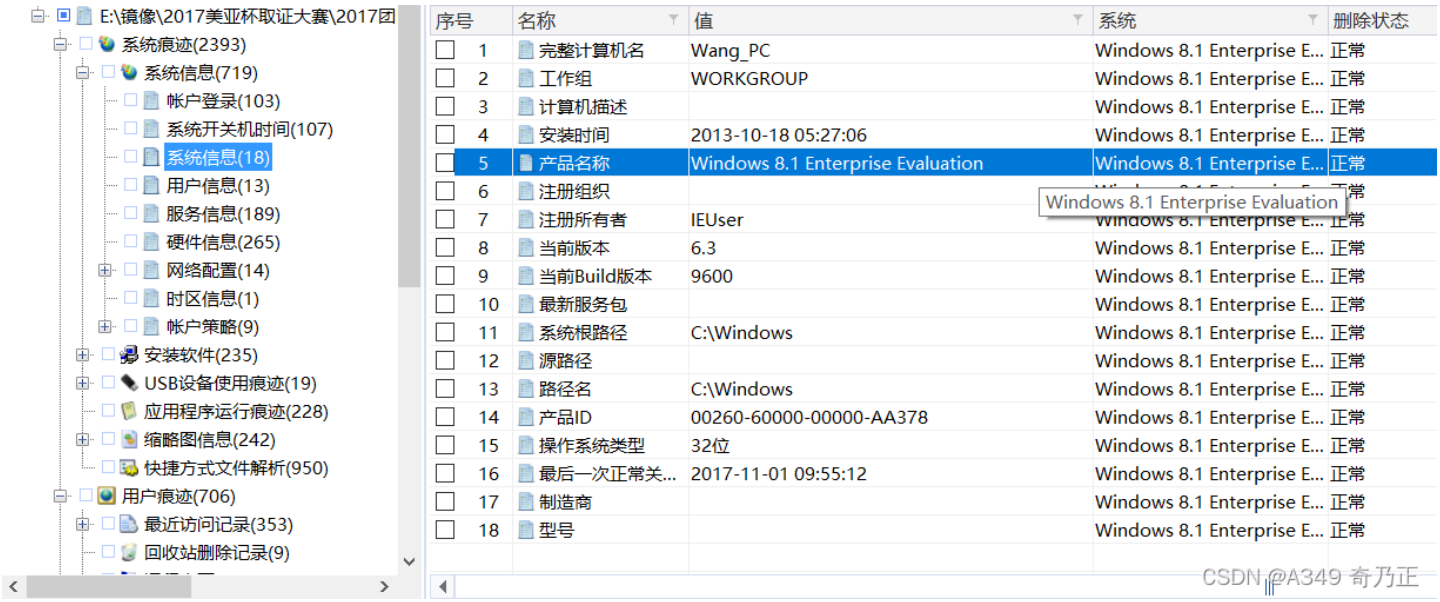
	62	用户“IEUSER " 的最后登入日期？
	A.	2013-08-22
	B.	2017-10-28
	C.	2017-10-30
√	D.	2017-11-01
	E.	2017-11-02

解析：见上题图



	63	硬盘的操作系统是什么？
	A.	windows7
√	B.	windows8
	C.	windows10
	D.	Linux Red Hat 7.1
	E.	MAC OS X

解析：见上题图



	64	根据执法机关调查所得，Eric曾经对暗网进行资料搜寻，并储存于电脑上。根据Eric 电脑上资料，那些来自暗网(Dark Web)并与洋葱网域(.onion)有关的信息，存放于哪个文件？
√	A.	好东西
	B.	暗东西
	C.	坏东西
	D.	宝贝
	E.	你的宝贝

解析：对答案进行搜索，发现好东西.docx符合要求

Deep web weapons Store Links

http://hhnovpxmqrw4xaqg.onion/ – Weapons – Black Market is a place for buy and sell guns, credit card and many other things in very optimal price hope this deep web sites will proving helpful for you, And you can find best Weapon here.

http://armoryohajjhou5m.onion/ – Weapons – Armory: This is great weapons store, where you can buy all type weapons by bitcoin. And mostly time I saw here, weapons price is good and cheap.

http://gunsjmzh2btr7lpy.onion/ – Deep web weapons – Guns Dark Markets: This deep web markets having good numbers of guns or any other weapons-related listings. Available some broad categories are Pistols, Assault Weapons, Full Auto Rifles, Submachine Guns, Sniper Rifles, Grenade Launchers, etc.

http://gunsdtk47tolcrre.onion/ – Weapons – UK Guns and Ammo Stores: Unique sites where you can deal with guns. Available products are Glock 19, Walther P99, Bullets for Glock 19, Walther P99

CSDN @A349 奇乃正

	65	上述的文件，提及了多少条洋葱网域(.onion)的信息？
	A.	1
	B.	2
	C.	3
√	D.	4
	E.	5

解析：见上题图

Deep web weapons Store Links

http://hhnovpxmqrw4xaqg.onion/ – Weapons – Black Market is a place for buy and sell guns, credit card and many other things in very optimal price hope this deep web sites will proving helpful for you, And you can find best Weapon here.

http://armoryohajjhou5m.onion/ – Weapons – Armory: This is great weapons store, where you can buy all type weapons by bitcoin. And mostly time I saw here, weapons price is good and cheap.

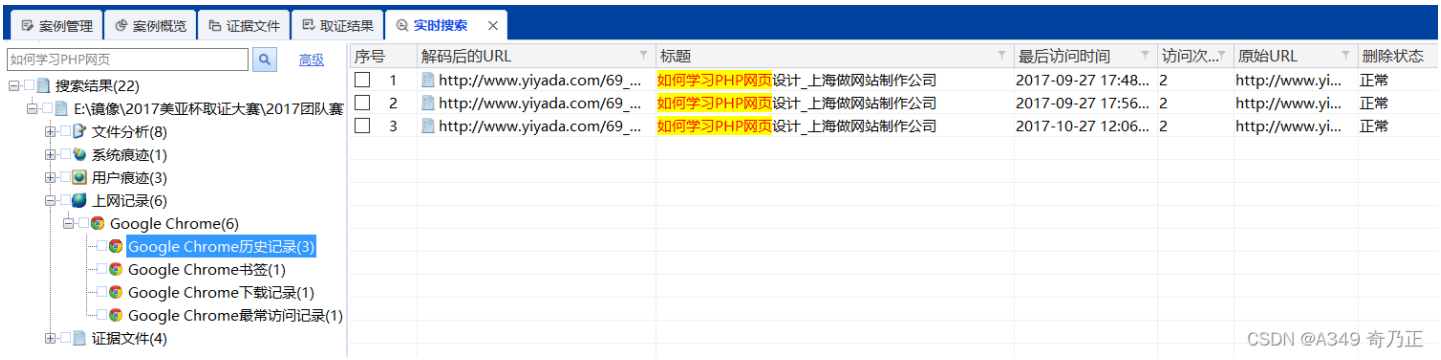
http://gunsjmzh2btr7lpy.onion/ – Deep web weapons – Guns Dark Markets: This deep web markets having good numbers of guns or any other weapons-related listings. Available some broad categories are Pistols, Assault Weapons, Full Auto Rifles, Submachine Guns, Sniper Rifles, Grenade Launchers, etc.

http://gunsdtk47tolcrre.onion/ – Weapons – UK Guns and Ammo Stores: Unique sites where you can deal with guns. Available products are Glock 19, Walther P99, Bullets for Glock 19, Walther P99

CSDN @A349 奇乃正

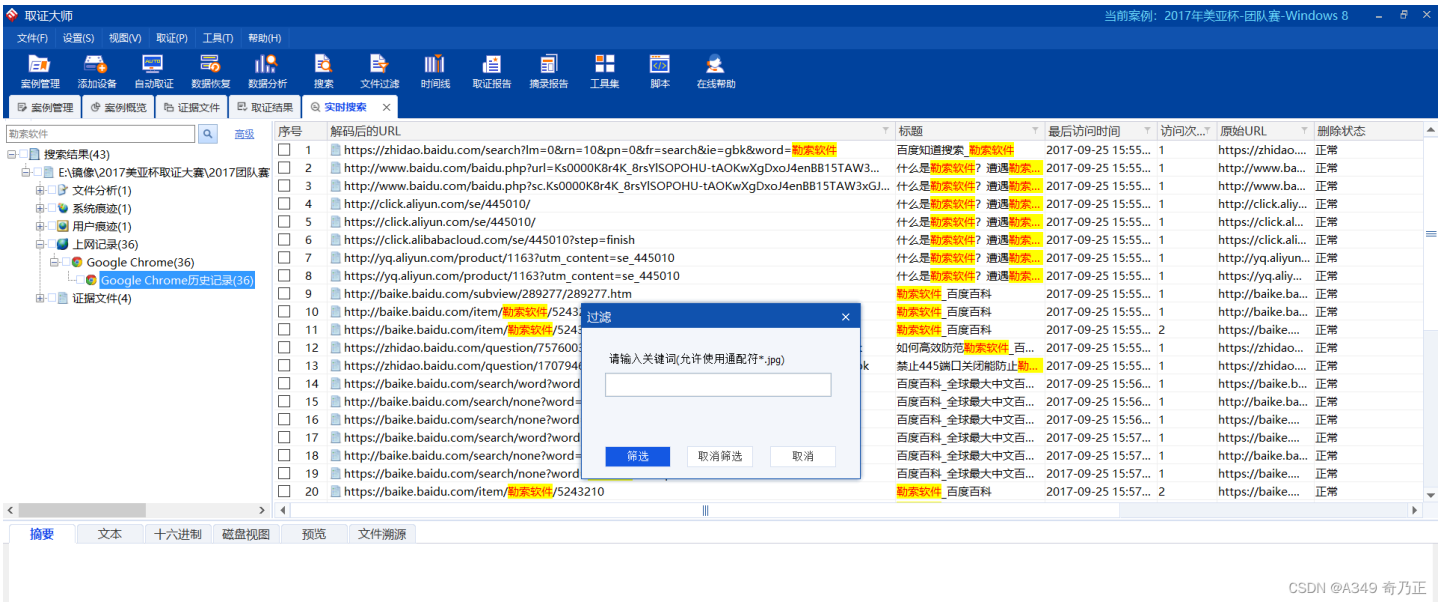
	66	Eric 曾在其电脑使用浏览器Chrome，浏览过一些有关“如何学习PHP网页计”的信息，下列哪项是相关的浏览记录？
√	A.	www.yiyada.com
	B.	www.hackdig.com/
	C.	www.carbonblack.com
	D.	www.antiy.com/
	E.	click.alibabacloud.com/

解析：搜索关键词“如何学习PHP网页”，在取证大师上网记录-Google Chrome-历史记录中可见。



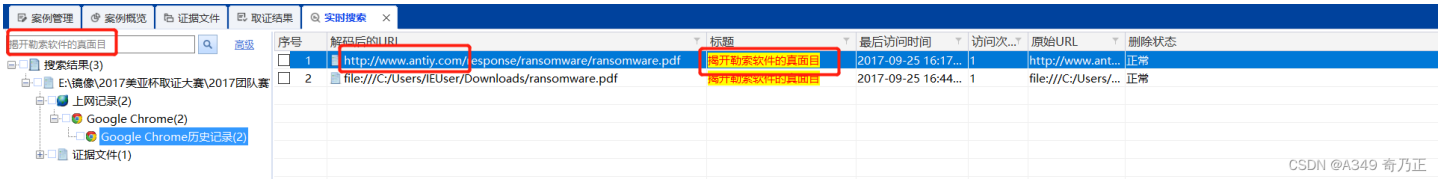
	67	Eric还曾在其电脑使用浏览器Chrome，搜集过一些有关勒索软件的信息，下列哪项不是相关的浏览记录？
	A.	www.hackdig.com/
	B.	click.aliyun.com/
√	C.	www.carbonblack.com
	D.	click.alibabacloud.com/
	E.	www.antiy.com/

解析：搜索关键词“勒索软件”，对解码后的URL进行过滤，没有发现C选项痕迹，故选C。



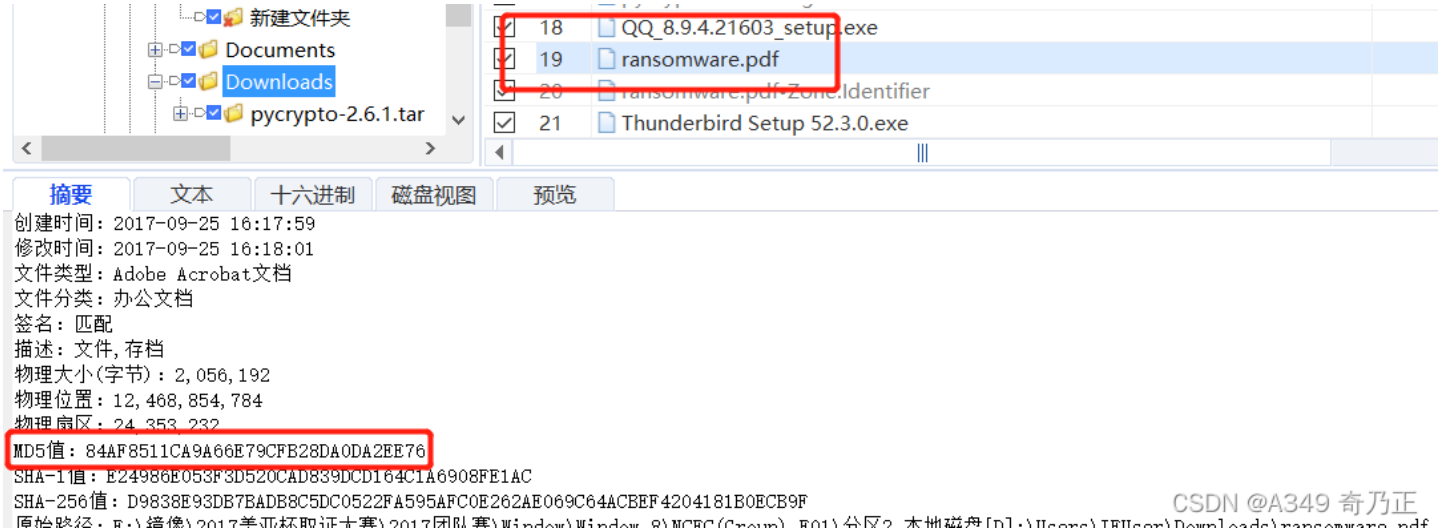
	68	根据执法机关调查所得，Eric更在上述其中一个网站下载了相关的勒索软件信息，是一份名为“揭开勒索软件的真面目”的文件。根据Eric电脑记录，是从哪个网站下载的？
	A.	www.hackdig.com/
	B.	click.aliyun.com/
	C.	www.carbonblack.com
	D.	click.alibabacloud.com/
√	E.	www.antiy.com/

解析：搜索关键词“揭开勒索软件的真面目”，发现上网记录中存在一份PDF，并且URL符合本题要求。



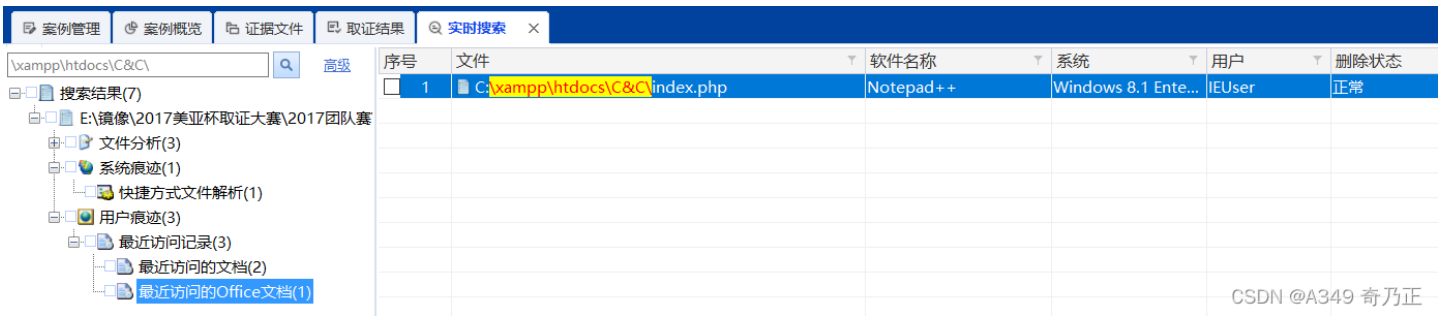
	69	续上题，该份名为“揭开勒索软件的真面目”文件的MD5哈希值(Hash value)是什么？
	A.	9110c96baa70c00acd8fbdfe2dc7c397
	B.	0258646764b1cb36ca2570090062b65c
	C.	ce38881d8f63a00973e6324bc1bf9245
	D.	703899985d881e2d103eb4fd1306be2e
√	E.	84af8511ca9a66e79cfb28da0da2ee76

解析：续上题，找到源文件，右键计算MD5值



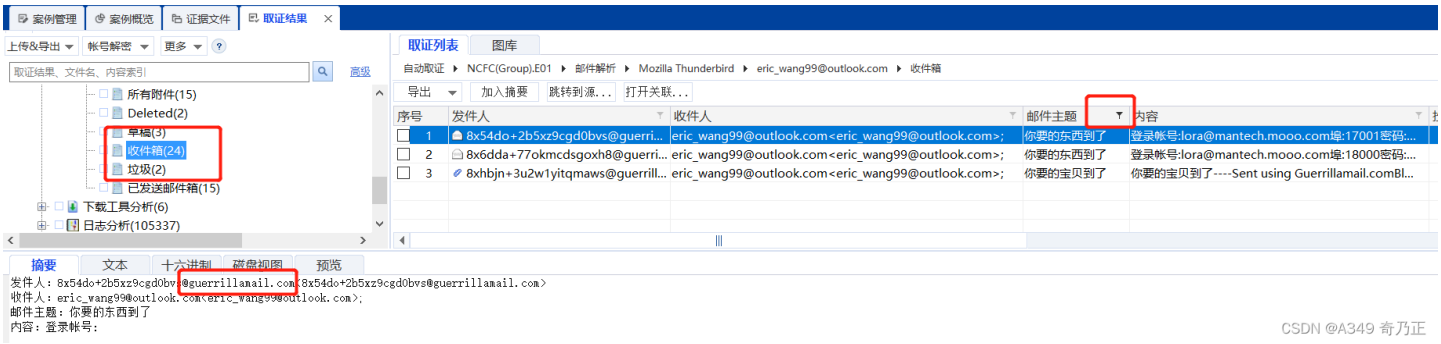
	70	Eric 曾在其电脑制造勒索网站，下列哪项是相关网站的首页位置？
	A.	\Windows\C&C\
√	B.	\xampp\htdocs\C&C\
	C.	\xampp\apache\C&C\
	D.	\xampp\httpd\C&C\
	E.	\inetpub\wwwroot\C&C\

解析：通过搜索答案的方法，只有B选项有结果，其余无结果。



	71	Eric 曾经收过一封有关mantech.mooo.com信息之电邮，标题为"你的东西到了"，根据Eric计算机记录，下列那个是发信人电邮地址之域名(Domain Name)?
√	A.	guerrillamail.com
	B.	guerrillomail.com
	C.	guerrillbmail.com
	D.	guerrillcmail.com
	E.	guerrilldmail.com

解析：进入邮件解析-收件箱，对邮件主题按关键词“你要的东西到了”进行过滤，得到相关信息，摘要内有发件人的详细域名。



CSDN @A349 奇乃正

	72	该封有关mantech.mooo.com信息的电邮，曾提及一个密码(Password)，是什么？
	A.	Fewer@4
	B.	Much@5
	C.	Less@6
√	D.	More@6
	E.	Echo@7

解析：接上题图，摘要可见。

CSDN @A349 奇乃正

	73	该封有关mantech.mooo.com信息的电邮，曾提及其相关连接埠，是多少？
	A.	11000及18000
	B.	10800及18000
	C.	16000及18000

	73	该封有关mantech.mooo.com信息的电邮，曾提及其相关连接埠，是多少？
	D.	17000及18000
√	E.	17001 及18000

解析：接上题图，摘要可见。

```
发件人：8x6dda+77okmcdsgoxh8@guerrillamail.com<8x6dda+77okmcdsgoxh8@guerrillamail.com>
收件人：eric_wang99@outlook.com<eric_wang99@outlook.com>;
邮件主题：你要的东西到了
内容：登录帐号:

lora@mantech.mooo.com

埠:

18000

密码:

More@6
```

CSDN @A349 奇乃正

```
发件人：8x54do+2b5xz9cgd0bvs@guerrillamail.com<8x54do+2b5xz9cgd0bvs@guerrillamail.com>
收件人：eric_wang99@outlook.com<eric_wang99@outlook.com>;
邮件主题：你要的东西到了
内容：登录帐号:

lora@mantech.mooo.com

埠:

17001

密码:

More@6
```

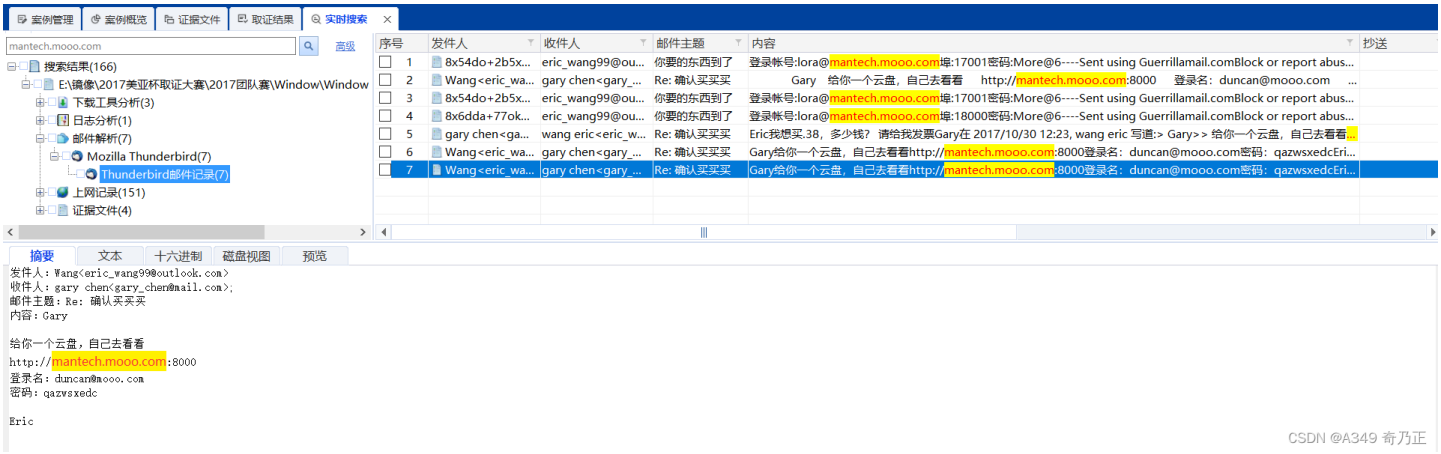
```
----
Sent using Guerrillamail.com
Block or report abuse: https://www.guerrillamail.com//abuse/?a=RFN9BjIXQroSOVeU%2F2sLfhvIRoST3do%3D
发送时间：2017-10-26 11:04:20
服务器接收时间：2017-10-26 11:04:23
附件个数：0
发件人IP：167.114.101.158; 51.15.63.98
邮件中转IP：10.152.68.59; 10.152.68.70; 10.152.69.198; 15.20.156.4; 167.114.101.158
删除状态：正常
```

CSDN @A349 奇乃正

	74	此外,亦有另一封有关mantech.mooo.com信息之电邮，曾提及一个云盘，而其相关端口，是多少？
√	A.	8000
	B.	8001
	C.	9000

	74	此外,亦有另一封有关mantech.mooo.com信息之电邮，曾提及一个云盘，而其相关端口，是多少？
	D.	9002
	E.	11000

解析：搜索关键词“mantech.mooo.com”，邮件解析-邮件记录中有符合题意的内容，可通过摘要查看详情。



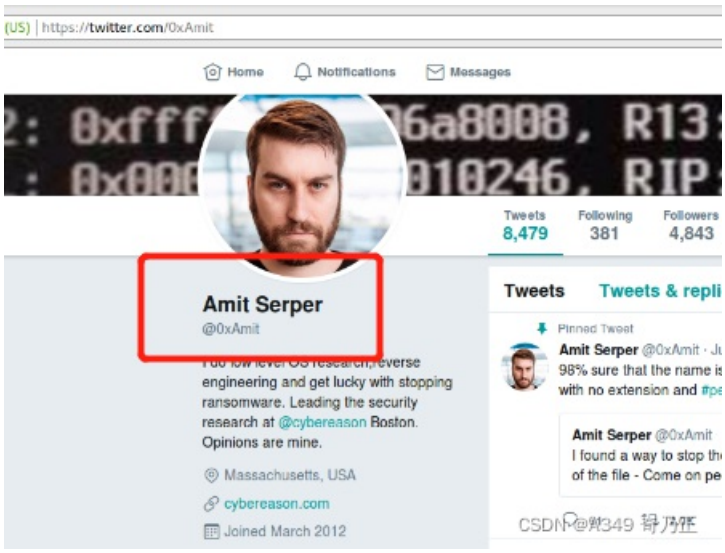
	75	Eric 曾经收过一封标题“你要的宝贝到了”的电邮，根据Eric电脑记录，下列哪个是发信人电邮地址(不包括域名)?
√	A.	8xhbjn+3u2w1yitqmaws
	B.	8xhbjn+3u2w1yitqmows
	C.	8xhbjn+3u2w1yitqmbws
	D.	8xhbjn+3u2w1yitqmsws
	E.	8xhbjn+3u2w1yitqmtws

解析：搜索关键词“你要的东西到了”，得到相关信息，摘要内有发件人的详细域名。

	76	上述该封标题“你要的宝贝到了”的电邮，附有一个电邮附件，详述了如何编写勒索软件。有关资料的提供者是谁？
	A.	Dave Ken
√	B.	Amit Serper
	C.	Amit Perper
	D.	Chris Kennedy

	76	上述该封标题“你要的宝贝到了”的电邮，附有一个电邮附件，详述了如何编写勒索软件。有关资料的提供者是谁？
	E.	David Kennedy

解析：密码爆破，密码：23456，打开压缩包后有一张图片，有Amity Serper。



	77	上述电邮附件，还提及过编写勒索软件相关原始码(Program Code)，其中显示Advanced Encryption Standard (AES)加密方法字眼的图片，其MD5哈希值(Hash value)是什么？
	A.	a93a6572335e37863f5d611293c6660
	B.	95c60bbc1cb267f85e51f99c2c9646f5
√	C.	0e20d5f091eac98f6e196dcda2c73837
	D.	ee2b59e91e829e3b3d350d8c14306dcb
	E.	f4b881e8a08d4bd40c5ee96ab3580bc8

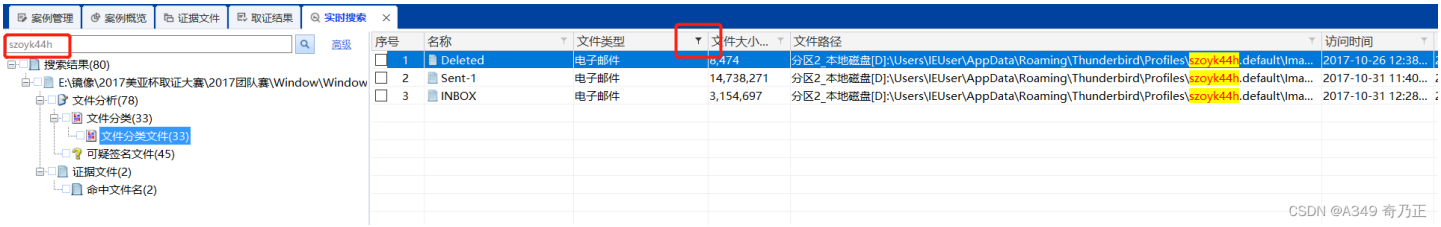
解析：仔细查找文件，发现图片“code.png”存在相关下内容并计算MD5.

```
import random
import string
import SintaRegistery
import SintaChangeWallpaper
from Crypto import Random
from Crypto.Cipher import AES
# Generates 25 random letters and numbers
# Used to help protect the private key
def random_key_mask(size=25, chars=string.ascii_lette
    return ''.join(random.choice(chars) for x in rang
```

CSDN @A349 奇乃正

	78	在个人竞赛中，Gary曾经收到一封来自电邮帐号 eric_wang99@outlook.com 的电邮，附加有三张与Apple iCloud有关的钓鱼网站相片。现经执法机关调查后，得知此电邮的发信人就是Eric。在Eric的电脑中，在哪位置可以找到电邮？
	A.	\Users\IEUser\AppData\Roaming\Thunderbird\Profiles\szoyi44h.default\ImapMail\imap-mail.outlook.com\Sent-1\网站价钱\
√	B.	\Users\IEUser\AppData\Roaming\Thunderbird\Profiles\szoyk44h.default\ImapMail\imap-mail.outlook.com\Sent-1\网站价钱\
	C.	\Users\IEUser\AppData\Roaming\Thunderbird\Profiles\szoyl44h.default\ImapMail\imap-mail.outlook.com\Sent-1\网站价钱\
	D	\Users\IEUser\AppData\Roaming\Thunderbird\Profiles\szoym44h.default\ImapMail\imap-mail.outlook.com\Sent-1\网站价钱\
	E.	\Users\IEUser\AppData\Roaming\Thunderbird\Profiles\szoyn44h.default\ImapMail\imap-mail.outlook.com\Sent-1\网站价钱\

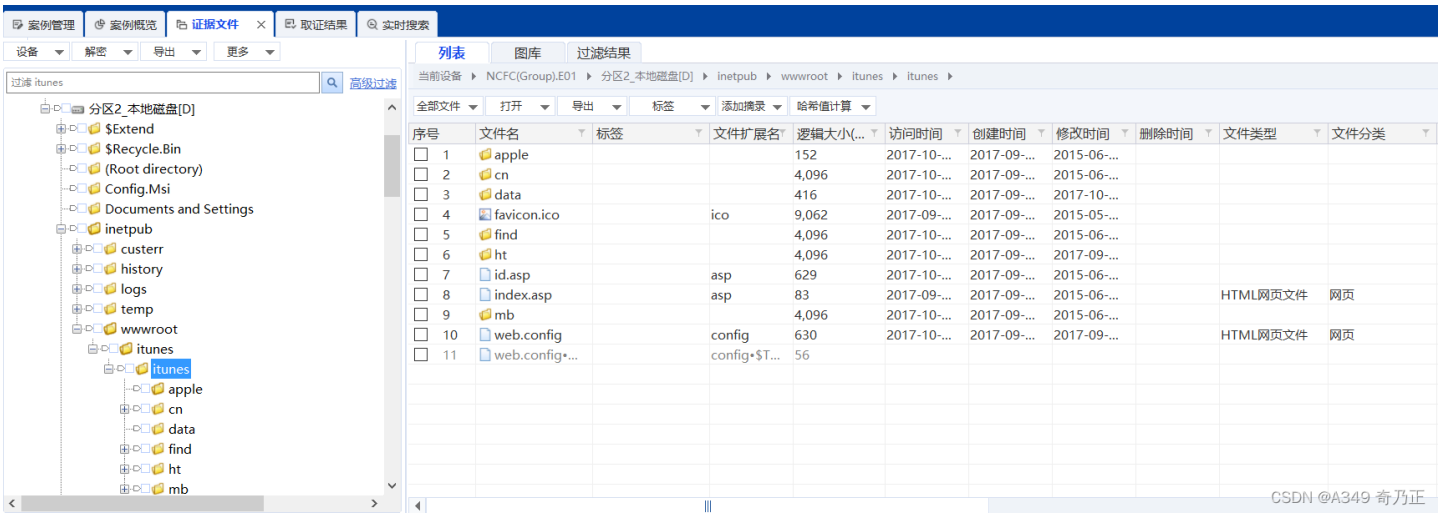
解析：搜索选项中不同部分，仅B选项有搜索结果，并在搜索结果中的文件分析-文件分类文件中，以“电子邮件”为关键词过滤文件，验证路径正确。



CSDN @A349 奇乃正

	79	续上题，在Eric的电脑中，在哪位置可以找到上述钓鱼网站资料？
	A.	\inetpub\wwwroot\itunes\itones\
	B.	\inetpub\wwwroot\itunes\itenes\
	C.	\inetpub\wwwroot\itunes\itanes\
√	D.	\inetpub\wwwroot\itunes\itunes\
	E.	\inetpub\wwwroot\itunes\itumes\

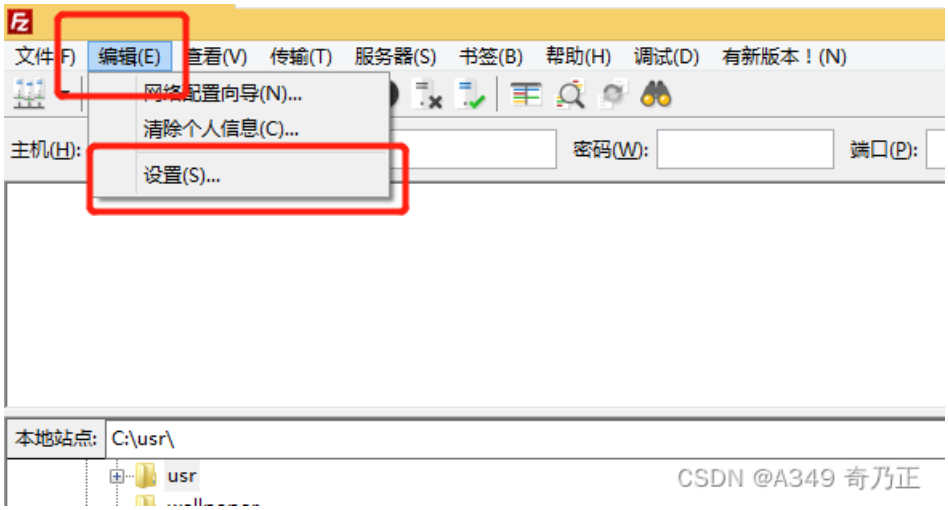
解析：搜索关键词“inetpub”，找到所属文件夹。



	80	Eric电脑储存了一个icloud 数据库供上述钓鱼网站所使用，根据相关记录，有多少IP地址是“登陆成功”?
	A.	13
	B.	14
	C.	15
√	D.	16
	E.	17

	81	根据执法机关调查所得，Eric是使用一个文件传输软件，进行网上远端文件存取，以逃避执法机关追查。下列哪个是相关软件。
	A.	vsftp
	B.	gftp
	C.	ProFTP
√	D.	Filezilla
	E.	Fire-FTP

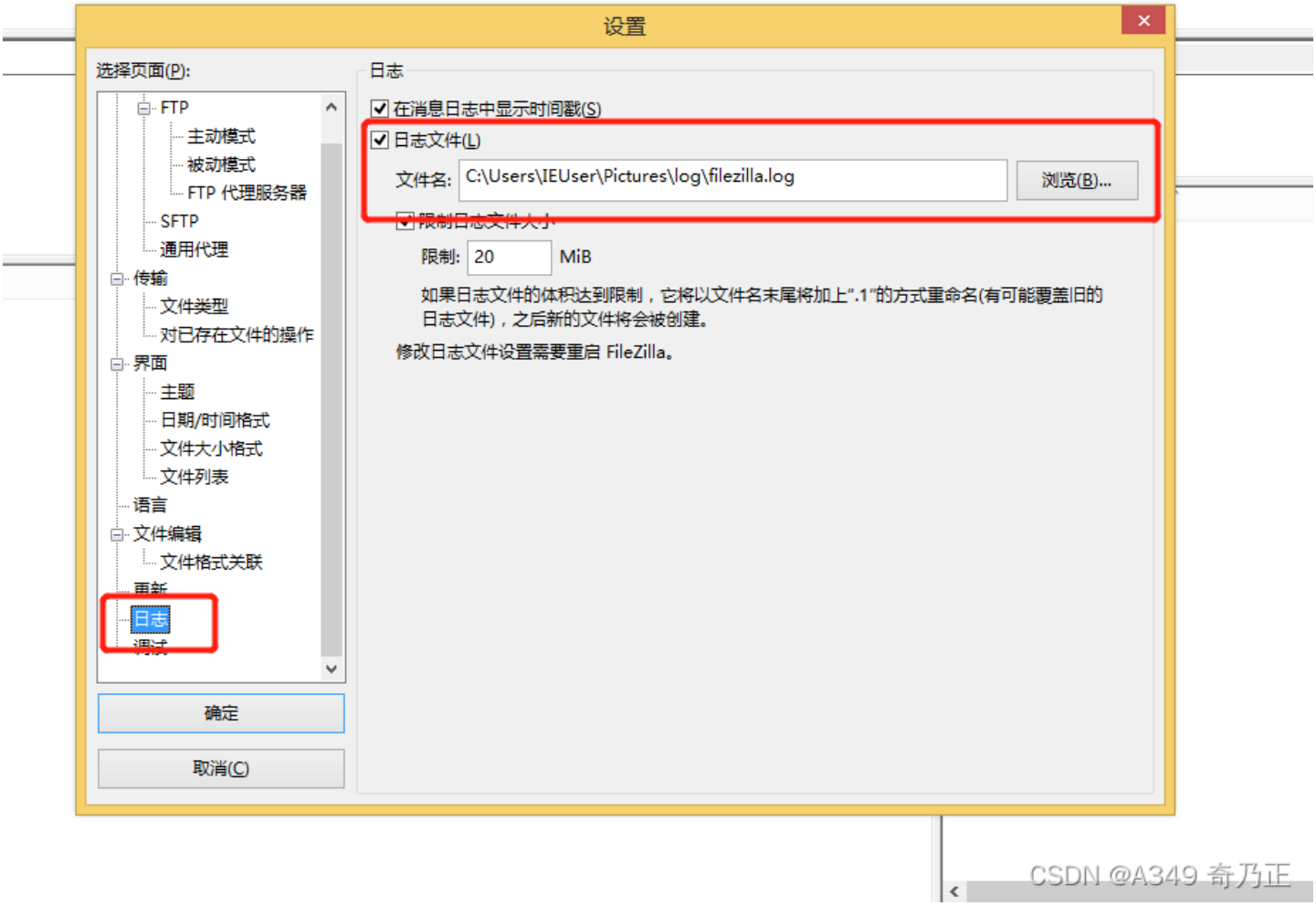
解析：火眼证据分析软件直接分析得出。



	82	上述文件传输软件相关的传输日志是储存在哪里？

	82	上述文件传输软件相关的传输日志是储存在哪里？
√	A.	Users\IEUser\Pictures\log\
	B.	Users\IEUser\Documents\
	C.	Users\IEUser\Pictures\log\
	D.	Users\IEUser\Music\
	E.	Program Files\

解析：在仿真软件中打开软件-设置-日志，可见日志保存路径。



CSDN @A349 奇乃正

	83	根据上述相关文件的传输日志显示，能成功登入的用户，有以下哪个用户？(请选择其中一项)
	i	amons
	ii	duncan
	iii	lora
	iv	warrior
	v	eric
	A.	i 及 ii
	B.	i, iii及 v

	83	根据上述相关文件的传输日志显示，能成功登入的用户，有以下哪个用户？(请选择其中一项)
	C.	i, iv及 v
√	D.	i, iii 及 iv
	E.	只有iv

解析：理论上是搜索关键词“Login successful”

更快的方式是搜索这五个用户名，然后得出答案

	84	根据上述成功登入的日志记录，该传输服务器的网址是什么？(请选择其中一项)
	A.	http://mantech.mooo.com:8000
√	B.	http://mantech.mooo.com:9000
	C.	http://mantech.mooo.com:17001
	D.	http://mantech.mooo.com:18000
√	E.	http://mantech.mooo.com:18001

解析：在日志中搜索关键词“成功”发现截图所示。

实际上更快的方式是搜索选项中的端口号带进去分析，

这道题我觉得B和E都是正确的

```
2017-10-27 16:52:52 3936 4 状态: 已登录
2017-10-27 16:52:52 3936 4 状态: 读取目录列表...
2017-10-27 16:52:52 3936 4 命令: PWD
2017-10-27 16:52:52 3936 4 响应: 257 "/home/lora" is the current directory
2017-10-27 16:52:52 3936 4 命令: TYPE I
2017-10-27 16:52:52 3936 4 响应: 200 Switching to Binary mode.
2017-10-27 16:52:52 3936 4 命令: PORT 192,168,123,128,200,129
2017-10-27 16:52:52 3936 4 响应: 500 Illegal PORT command.
2017-10-27 16:52:52 3936 4 命令: PASV
2017-10-27 16:52:52 3936 4 响应: 227 Entering Passive Mode (192,168,122,157,250,122).
2017-10-27 16:52:52 3936 4 状态: 服务器发回了不可路由的地址。使用服务器地址代替。
2017-10-27 16:52:52 3936 4 命令: LIST
2017-10-27 16:52:57 3936 3 错误: 20 秒后无活动，连接超时
2017-10-27 16:52:57 3936 3 错误: 读取目录列表失败
2017-10-27 16:52:57 3936 3 状态: 已从服务器断开
2017-10-27 16:52:57 3936 3 状态: 正在解析 mantech.mooo.com 的地址
2017-10-27 16:52:57 3936 3 状态: 正在连接 223.17.250.208:18001...
2017-10-27 16:52:57 3936 3 状态: 连接建立，等待欢迎消息...
2017-10-27 16:52:57 3936 3 响应: 220 (vsFTPd 3.0.3)
2017-10-27 16:52:57 3936 3 命令: AUTH TLS
2017-10-27 16:52:57 3936 3 响应: 530 Please login with USER and PASS.
2017-10-27 16:52:57 3936 3 命令: AUTH SSL
2017-10-27 16:52:57 3936 3 响应: 530 Please login with USER and PASS.
2017-10-27 16:52:57 3936 3 状态: 不安全的服务器，不支持 FTP over TLS。
2017-10-27 16:52:57 3936 3 命令: USER lora
2017-10-27 16:52:57 3936 3 响应: 331 Please specify the password.
2017-10-27 16:52:57 3936 3 命令: PASS ******
2017-10-27 16:52:57 3936 4 错误: 无法建立数据连接: ECONNREFUSED - 连接被服务器拒绝
2017-10-27 16:52:57 3936 3 响应: 230 Login successful.
2017-10-27 16:52:57 3936 3 状态: 服务器不支持非 ASCII 字符。
2017-10-27 16:52:57 3936 3 状态: 已登录
2017-10-27 16:52:57 3936 3 状态: 读取目录列表...
2017-10-27 16:52:57 3936 3 命令: PWD
2017-10-27 16:52:57 3936 3 响应: 257 "/home/lora" is the current directory
2017-10-27 16:52:57 3936 3 命令: TYPE I
```

CSDN @A349 奇乃正

```
2017-10-30 20:10:57 3096 1 命令: ls
2017-10-30 20:10:57 3096 1 状态: Listing directory /home/amons/Coding/invoice/build
2017-10-30 20:10:57 3096 1 状态: 列出"/home/amons/Coding/invoice/build"的目录成功
2017-10-30 20:11:18 3096 4 状态: 正在连接 mantech.mooo.com:9000...
2017-10-30 20:11:18 3096 4 响应: fzSftp started, protocol_version=8
2017-10-30 20:11:18 3096 4 命令: open "amons@mantech.mooo.com" 9000
2017-10-30 20:11:18 3096 4 命令: 信任新的主机密钥: 一次
2017-10-30 20:11:18 3096 4 命令: Pass: ********
2017-10-30 20:11:18 3096 4 状态: Connected to mantech.mooo.com
2017-10-30 20:11:18 3096 4 状态: 开始下载 /home/amons/Coding/invoice/pdf.ico
2017-10-30 20:11:18 3096 4 命令: cd "/home/amons/Coding/invoice"
2017-10-30 20:11:18 3096 4 响应: New directory is: "/home/amons/Coding/invoice"
2017-10-30 20:11:18 3096 4 命令: get "pdf.ico" "C:\usr\pdf.ico"
2017-10-30 20:11:18 3096 4 命令: remote:/home/amons/Coding/invoice/pdf.ico => local:C:\usr\pdf.ico
2017-10-30 20:11:18 3096 4 状态: 文件传输成功，传输了 32,768 字节 (用时1 秒)
```

CSDN @A349 奇乃正

	85	根据上述相关文件的传输日志显示，能成功从服务器下载文件的用户，是以下哪个用户？
√	A.	amons
	B.	duncan
	C.	lora
	D.	warrior
	E.	eric

解析：找到截图所示。

```
2017-10-30 20:10:57 3096 1 状态: Listing directory /home/amons/Coding/invoice/build
2017-10-30 20:10:57 3096 1 状态: 列出"/home/amons/Coding/invoice/build"的目录成功
2017-10-30 20:11:18 3096 4 状态: 正在连接 mantech.mooo.com:9000...
2017-10-30 20:11:18 3096 4 响应: fzSftp started, protocol_version=8
2017-10-30 20:11:18 3096 4 命令: open "amons@mantech.mooo.com" 9000
2017-10-30 20:11:18 3096 4 命令: 信任新的主机密钥: 一次
2017-10-30 20:11:18 3096 4 命令: Pass: ********
2017-10-30 20:11:18 3096 4 状态: Connected to mantech.mooo.com
2017-10-30 20:11:18 3096 4 状态: 开始下载 /home/amons/Coding/invoice/pdf.ico
2017-10-30 20:11:18 3096 4 命令: cd "/home/amons/Coding/invoice"
2017-10-30 20:11:18 3096 4 响应: New directory is: "/home/amons/Coding/invoice"
2017-10-30 20:11:18 3096 4 命令: get "pdf.ico" "C:\usr\pdf.ico"
2017-10-30 20:11:18 3096 4 命令: remote:/home/amons/Coding/invoice/pdf.ico => local:C:\u
2017-10-30 20:11:18 3096 4 状态: 文件传输成功，传输了 32,768 字节(用时1秒)
```

CSDN @A849 奇乃正

	86	根据上述相关文件的传输日志显示，用户是使用了什么传输网址最后成功从服务器下载文件？
	A.	http://mantech.mooo.com:8000
√	B.	http://mantech.mooo.com:9000
	C.	http://mantech.mooo.com:17001
	D.	http://mantech.mooo.com:18000
	E.	http://mantech.mooo.com:18001

解析：查看日志文件，截图所示。

```
2017-10-30 20:11:18 3096 4 状态: 正在连接 mantech.mooo.com:9000...
2017-10-30 20:11:18 3096 4 响应: fzSftp started, protocol_version=8
2017-10-30 20:11:18 3096 4 命令: open "amons@mantech.mooo.com" 9000
2017-10-30 20:11:18 3096 4 命令: 信任新的主机密钥: 一次
2017-10-30 20:11:18 3096 4 命令: Pass: ********
2017-10-30 20:11:18 3096 4 状态: Connected to mantech.mooo.com
2017-10-30 20:11:18 3096 4 状态: 开始下载 /home/amons/Coding/invoice/pdf.ico
2017-10-30 20:11:18 3096 4 命令: cd "/home/amons/Coding/invoice"
2017-10-30 20:11:18 3096 4 响应: New directory is: "/home/amons/Coding/invoice"
```

	87	根据Eric电脑的浏览网页记录，他是何时浏览私有云盘http://mantech.mooo.com:8000?
	A.	2017-10-29
√	B.	2017-10-30
	C	2017-10-31
	D.	2017-11-01
	E.	2017-11-02

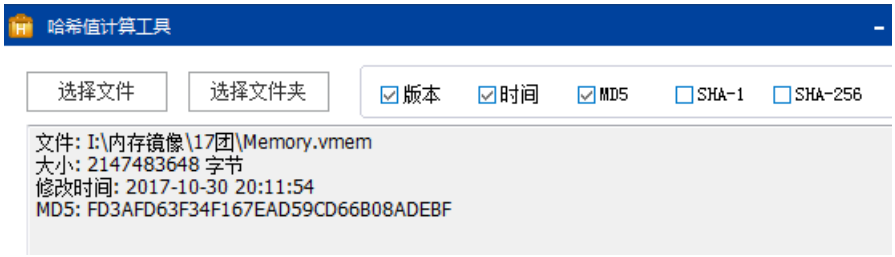
解析：搜索关键词http://mantech.mooo.com:8000，历史记录中可得最后访问时间。

Win8 – Memory

	88	执法机关曾在Eric的电脑进行现场搜证并检取其虚拟内存，放在下列位置中: Users\IEUser\Desktop\RAM\ , 文件名称:Memory.vmem。下列哪项是其MD5哈希值？
	A.	3A70A392F8FF1DE83F8CAE94C4E71427
	B.	5F1BDEB87EE9F710C90CFB3A0BB01616
	C.	F68778AE77C4E4B88212B179C4622FC4

	88	执法机关曾在Eric的电脑进行现场搜证并检取其虚拟内存，放在下列位置中: Users\IEUser\Desktop\RAM\ , 文件名称:Memory.vmem。下列哪项是其MD5哈希值？
	D.	16160CFB3A0BB016166A0BB016166167
√	E.	FD3AFD63F34F167EAD59CD66B08ADEBF

解题：使用取证大师计算其哈希值



	89	在该段内存中，共运行了多少个进程(以独立程序ID计算)?
	A.	16
	B.	25
	C.	48
√	D.	54
	E.	62

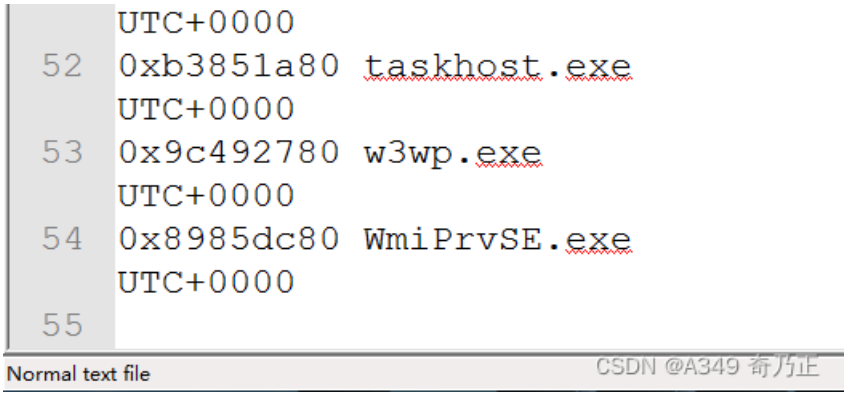
解题：使用volatility软件，

方法一：

命令：

volatility -f Me.vmem --profile=Win81u1x86 pslist > pslist.txt

输出文件的头两行说明部分删掉，即最后一行是进程数的总数量

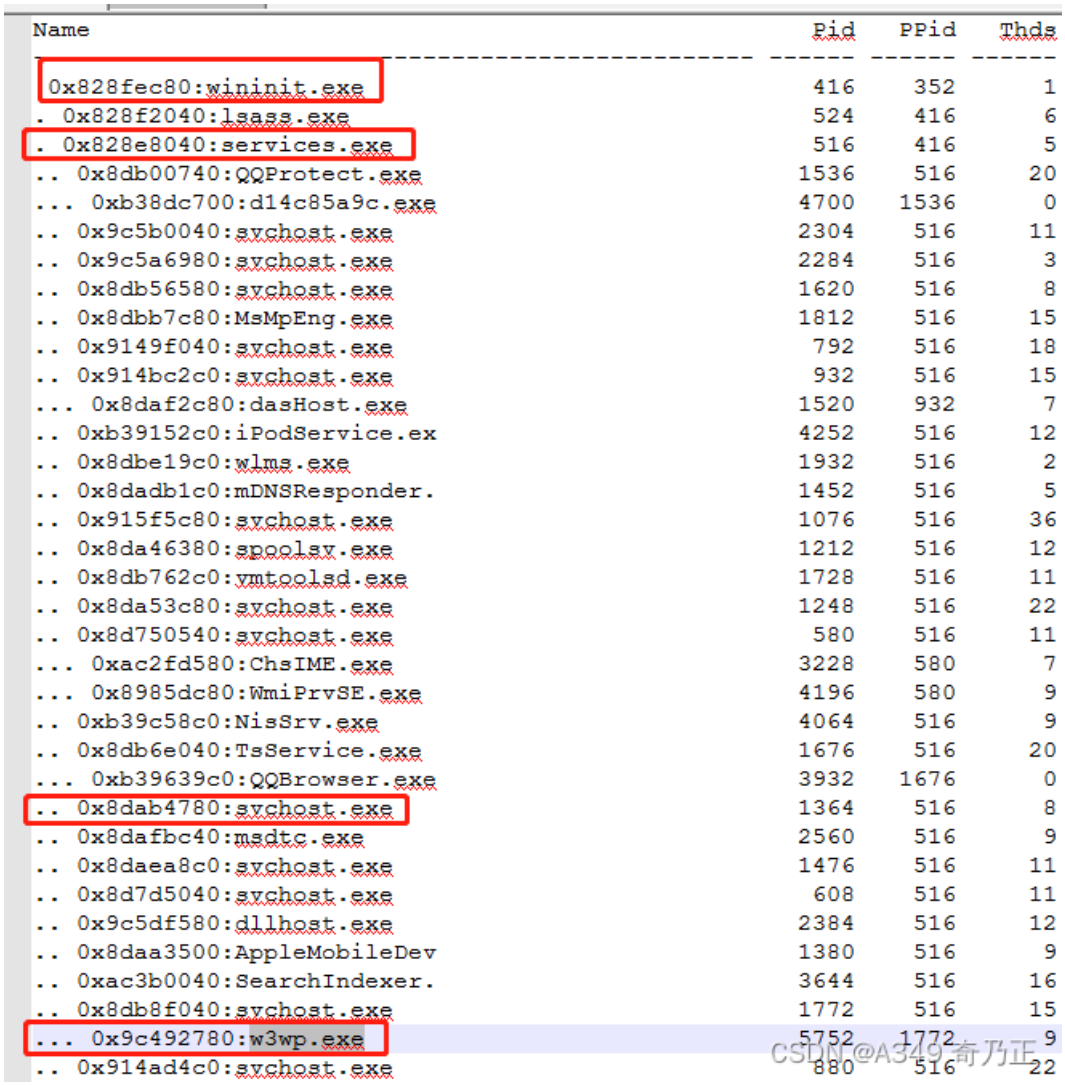


方法二：

使用取证大师内存镜像分析工具找到54个进程

	90	就进程w3wp.exe而言，下列哪项是该程序产生次序？
	A.	wininit.exe >services.exe > w3wp.exe > svchost.exe
	B.	smss.exe >services.exe > svchost.exe > w3wp.exe
√	C.	wininit.exe >services.exe > svchost.exe > w3wp.exe
	D.	csrss.exe >> svchost.exe > services.exe > w3wp.exe
	E.	System >services.exe > svchost.exe > w3wp.exe

解题：volatility -f Me.vmem --profile=Win81u1x86 pstree > pstree.txt



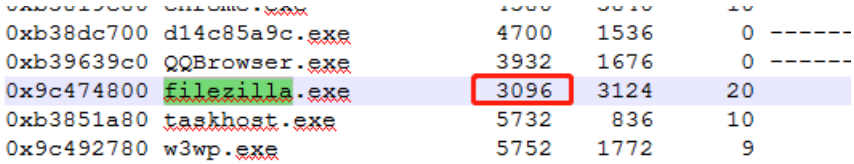
```
Name                                                 Pid   PPid   Thds
---------------------------------------------------- ------ ------ ------
0x828fec80:wininit.exe                                416    352      1
. 0x828f2040:lsass.exe                                524    416      6
. 0x828e8040:services.exe                             516    416      5
.. 0x8db00740:QQProtect.exe                          1536    516     20
... 0xb38dc700:d14c85a9c.exe                         4700   1536      0
.. 0x9c5b0040:svchost.exe                            2304    516     11
.. 0x9c5a6980:svchost.exe                            2284    516      3
.. 0x8db56580:svchost.exe                            1620    516      8
.. 0x8dbb7c80:MsMpEng.exe                            1812    516     15
.. 0x9149f040:svchost.exe                             792    516     18
.. 0x914bc2c0:svchost.exe                             932    516     15
... 0x8daf2c80:dasHost.exe                           1520    932      7
.. 0xb39152c0:iPodService.ex                         4252    516     12
.. 0x8dbe19c0:wlms.exe                               1932    516      2
.. 0x8dadb1c0:mDNSResponder.                         1452    516      5
.. 0x915f5c80:svchost.exe                            1076    516     36
.. 0x8da46380:spoolsv.exe                            1212    516     12
.. 0x8db762c0:vmtoolsd.exe                           1728    516     11
.. 0x8da53c80:svchost.exe                            1248    516     22
.. 0x8d750540:svchost.exe                             580    516     11
... 0xac2fd580:ChsIME.exe                            3228    580      7
... 0x8985dc80:WmiPrvSE.exe                          4196    580      9
.. 0xb39c58c0:NisSrv.exe                             4064    516      9
.. 0x8db6e040:TsService.exe                          1676    516     20
... 0xb39639c0:QQBrowser.exe                         3932   1676      0
.. 0x8dab4780:svchost.exe                            1364    516      8
.. 0x8dafbc40:msdtc.exe                              2560    516      9
.. 0x8daea8c0:svchost.exe                            1476    516     11
.. 0x8d7d5040:svchost.exe                             608    516     11
.. 0x9c5df580:dllhost.exe                            2384    516     12
.. 0x8daa3500:AppleMobileDev                         1380    516      9
.. 0xac3b0040:SearchIndexer.                         3644    516     16
.. 0x8db8f040:svchost.exe                            1772    516     15
... 0x9c492780:w3wp.exe                              5752   1772      9
.. 0x914ad4c0:svchost.exe                             880    516     22
```

CSDN @A349 奇乃正

	91	根据调查资料，Eric总是使用filezilla软件上传/下载文件。filezilla的程序ID是什么？
	A.	4
	B.	780
	C.	820
√	D.	3096
	E.	3228

解题: 命令：

volatility -f Me.vmem --profile=Win81u1x86 pslist > pslist.txt



```
0xb38dc700 d14c85a9c.exe          4700   1536      0 ------
0xb39639c0 QQBrowser.exe          3932   1676      0 ------
0x9c474800 filezilla.exe          3096   3124     20
0xb3851a80 taskhost.exe           5732    836     10
0x9c492780 w3wp.exe               5752   1772      9
```

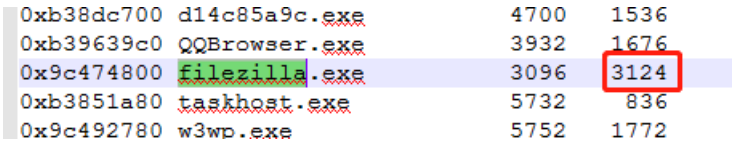
	92	上述filezilla进程的父程序(Parent PID) 是什么？
	A.	516
	B.	1536
	C.	1676

	92	上述filezilla进程的父程序(Parent PID) 是什么？
	D.	2284
√	E.	3124

解题：

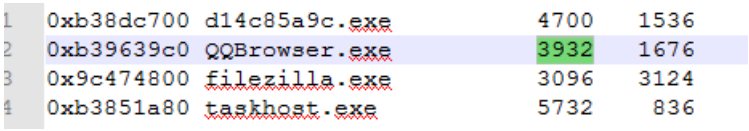
命令：

volatility -f Me.vmem --profile=Win81u1x86 pslist > pslist.txt



	93	你知道程序ID:3932是什么进程(process)吗？
	A.	winlogon.exe
√	B.	QQBrowser.exe
	C.	QQProtect.exe
	D.	svchost.exe
	E.	chrome.exe

解题：方法同上题

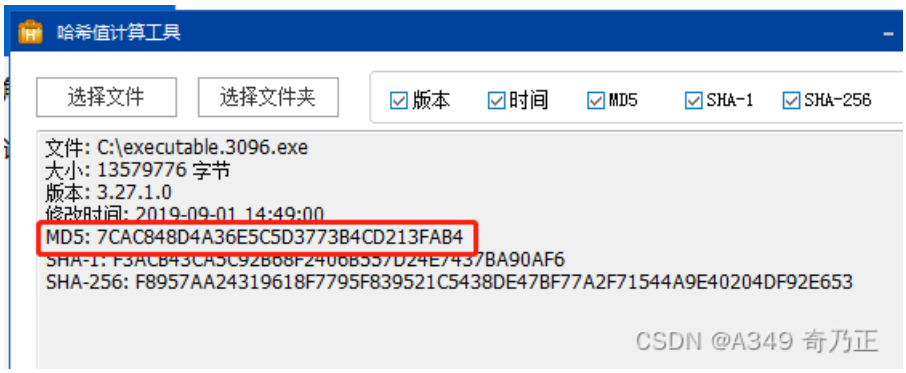


	94	请从该段内存中提取(E√tract)上述filezilla进程的原来执行档 - filezilla.e√e文件，并计算其md5哈希值(hash value)。下列哪行是该md5哈希值？
	A.	43502d07de3d31f05f1623b76c47a58e
√	B.	7cac848d4a36e5c5d3773b4cd213fab4
	C.	2717eae9129e3943d33c639825654425
	D.	98eb240853589172c82e3d7935e9b7ba
	E.	147fc1da6b0a752be633dcb20553450

解题：使用命令

volatility -f Me.vmem --profile=Win81u1x86 procdump -p pid -D /下载的路径

再将导出来的文件计算md5值



	95	根据上述的取回的文件filezilla.exe，它在执行时会呼叫多少个动态连结函式库(Dynamic Linked Library)?
	A.	32
	B.	56
	C.	73
√	D.	82
	E.	98

解题：

命令：

volatility -f Me.vmem --profile=Win81u1x86 dlllist > dlllist.txt

导出的文件计算头减去尾部的行数，得82

```
3032  0x72f80000     0x42000         0x0 C:\Windows\System32\UIAnimation.dll
3033  0x731c0000    0x181000         0x0 C:\Windows\system32\dwrite.dll
3034  0x74d50000     0x4b000         0x0 C:\Windows\system32\mswsock.dll
3035  0x74bc0000     0x7e000         0x0 C:\Windows\SYSTEM32\DNSAPI.dll
3036  0x6ddd0000     0x21000         0x0 C:\Program Files\Bonjour\mdnsNSP.dll
3037  0x71f90000     0x20000         0x0 C:\Windows\SYSTEM32\Iphlpapi.DLL
3038  0x71dc0000      0x8000         0x0 C:\Windows\SYSTEM32\WINNSI.DLL
3039  0x6dda0000      0x8000         0x0 C:\Windows\System32\rasadhlp.dll
3040  0x71ba0000     0x46000         0x0 C:\Windows\System32\fwpuclnt.dll
3041  0x730a0000     0x50000         0x0 C:\Windows\System32\oleacc.dll
3042  0x73600000    0x1d9000         0x0 C:\Windows\system32\d3d11.dll
3043  0x73580000     0x69000         0x0 C:\Windows\system32\dxgi.dll
3044  0x66ed0000    0x218000         0x0 C:\Windows\SYSTEM32\D3D10Warp.dll
3045  0x73ac0000     0x46000         0x0 C:\Windows\SYSTEM32\dcomp.dll
3046  ********************************************************************************
```

CSDN @A349 奇乃正

```
2958  filezilla.exe pid:   3096
2959  Command line : "C:\Program Files\FileZilla FTP Client\filezilla.exe"
2960
2961
2962  Base             Size  LoadCount Path  3045-2963
2963  ---------- ---------- ---------- ----
2964  0x00400000   0xd30000         0x0 C:\Program Files\FileZilla FTP Client\filezilla.exe
2965  0x77ba0000   0x16a000         0x0 C:\Windows\SYSTEM32\ntdll.dll
2966  0x75a40000   0x100000         0x0 C:\Windows\system32\KERNEL32.DLL
2967  0x756e0000    0xd9000         0x0 C:\Windows\system32\KERNELBASE.dll
2968  0x760b0000    0x7c000         0x0 C:\Windows\system32\ADVAPI32.dll
2969  0x73b10000   0x206000         0x0 C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf
2970  0x75b40000    0x9b000         0x0 C:\Windows\system32\COMDLG32.DLL
2971  0x75550000   0x188000         0x0 C:\Windows\system32\CRYPT32.dll
2972  0x76210000   0x110000         0x0 C:\Windows\system32\GDI32.dll
2973  0x6c6c0000    0x16000         0x0 C:\Windows\SYSTEM32\MPR.DLL
2974  0x75be0000    0xc3000         0x0 C:\Windows\system32\msvcrt.dll
2975  0x72410000    0x13000         0x0 C:\Windows\SYSTEM32\NETAPI32.dll
2976  0x75e80000     0x5000         0x0 C:\Windows\system32\Normaliz.dll
2977  0x76360000   0x129000         0x0 C:\Windows\system32\ole32.dll
2978  0x77b00000    0x97000         0x0 C:\Windows\system32\OLEAUT32.dll
2979  0x75350000    0x40000         0x0 C:\Windows\SYSTEM32\POWRPROF.dll
2980  0x764a0000   0x12bb000         0x0 C:\Windows\system32\SHELL32.dll
2981  0x758e0000   0x155000         0x0 C:\Windows\system32\USER32.dll
2982  0x70f60000    0x23000         0x0 C:\Windows\SYSTEM32\WINMM.DLL
2983  0x76130000    0x4f000         0x0 C:\Windows\system32\WS2_32.dll
```

CSDN @A349 奇乃正

	96	在Eric的电脑中，还储存有一个同名的文件filezilla.exe，你能找到该文件的md5哈希值(hash value)吗？
	A.	43502d07de3d31f05f1623b76c47a58e
	B.	7cac848d4a36e5c5d3773b4cd213fab4
√	C.	2717eae9129e3943d33c639825654425
	D.	98eb240853589172c82e3d7935e9b7ba
	E.	147fc1da6b0a752be633dcb20553450

解题：

```
文件名：filezilla.exe
文件扩展名：exe
逻辑大小(字节)：13,594,280
访问时间：2017-11-01 10:06:11
创建时间：2017-08-15 00:08:36
修改时间：2017-08-15 00:08:36
签名：匹配
描述：文件，存档
物理大小(字节)：13,594,624
物理位置：11,829,260,288
物理扇区：23,104,024
MD5值：2717EAE9129E3943D33C639825654425
SHA-1值：500F1D89395F971F0CD84D8F7BD25AD308DE4E25
SHA-256值：AD8A0A5DB9C78DBA8D1FB31A15BEF59C59C9C15549D00E6496005D87F803B0A1
原始路径：E:\镜像\2017美亚杯取证大赛\2017团队赛\Window\Window 8\NCFC(Group).E01\分区2_本地磁盘[D]:\Program Files\FileZilla FTP Client\filezilla.exe
完整路径：2017年美亚杯-团队赛-Windows 8\E:\镜像\2017美亚杯取证大赛\2017团队赛\Window\Window 8\NCFC(Group).E01\分区2_本地磁盘[D]:\Program Files\FileZilla FTP Client\filezilla.exe
```

CSDN @A349 奇乃正

	97	该段内存中有多少个连接埠与svchost.exe有关？
	A.	3
	B.	4
	C.	5
	D.	6
√	E.	7

解题：

命令：

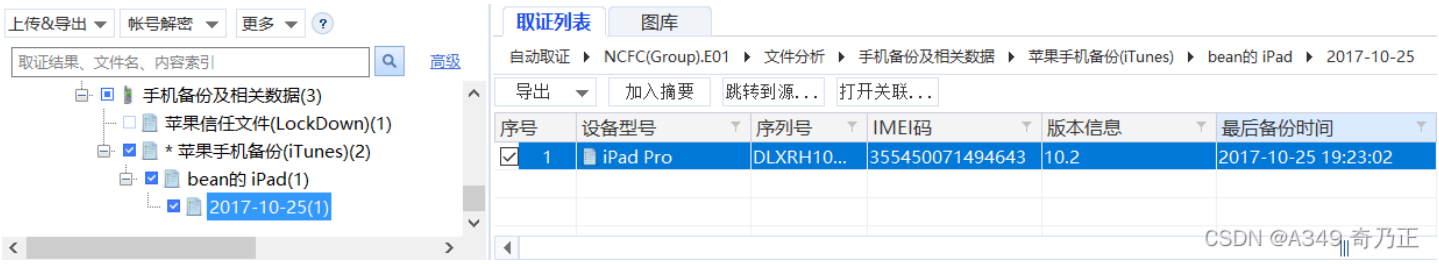
volatility -f Me.vmem --profile=Win81u1x86 netscan > netscan.txt

在导出的txt文档中进行分析

(Bonus) iPad 7

	98	Eric有一个苹果可携式设备，并备份到电脑，密码是wangapple，最后备份的日期是什么？
	A.	2017-10-22
	B.	2017-10-23
	C.	2017-10-24
√	D.	2017-10-25
	E.	2017-10-26

解析：在取证大师－文件分析－手机备份及相关数据－苹果手机备份中可见



	99	该苹果可携式设备，是什么型号？
	A.	MLQ32ZP/C
	B.	MLQ64ZP/B
	C.	MLQ32ZP/B
	D.	MLQ64ZP/A
√	E.	MLQ32ZP/A

	100	该苹果可携式设备名称是什么？
	A.	bean的 iPhone

	100	该苹果可携式设备名称是什么？
√	B.	bean的 iPad
	C.	bean的iPad Mini
	D.	bean的iPod
	E.	bean的iPod Touch

解析：在手机大师－文件信息－基本信息中可见

序号	信息	内容
3	本机号码2	
4	创建时间	2019-08-31 15:50:55
5	创建版本	14C92
6	设备名	bean的 iPad
7	GUID	754EF524A0760423B04D6C81CDCD0626
8	ICCID	89013802297038093133
9	IMEI	355450071494643
10	最后备份日期	2017-10-25 19:23:02
11	手机型号	未知
12	系统版本	10.2
13	序列号	DLXRH10JGXQ4
14	设备ID	6F7E653CC83768FF0A5F07724064D85FA6D4FD2B
15	时区	GMT+08:00
16	设备名称	6f7e653cc83768ff0a5f07724064d85fa6d4fd2b
17	持有人编号	
18	证件类型	身份证

CSDN @A349 奇乃正

	101	该苹果可携式设备序号是什么？
	A.	4D85FA6D4FD2
	B.	6F7E653CCSD48
	C.	3CCSD46F7E653
√	D.	DLXRH10JGXQ4
	E.	10JGXQ4DLXRH

解析：在手机大师－文件信息－基本信息中可见

序号	信息	内容
5	创建版本	14C92
6	设备名	bean的 iPad
7	GUID	754EF524A0760423B04D6C81CDCD0626
8	ICCID	89013802297038093133
9	IMEI	355450071494643
10	最后备份日期	2017-10-25 19:23:02
11	手机型号	未知
12	系统版本	10.2
13	序列号	DLXRH10JGXQ4
14	设备ID	6F7E653CC83768FF0A5F07724064D85FA6D4FD2B
15	时区	GMT+08:00
16	设备名称	6f7e653cc83768ff0a5f07724064d85fa6d4fd2b
17	持有人编号	
18	证件类型	身份证
19	证件编号	
20	设备性质	无主或其它性质手机

CSDN @A349 奇乃正

	102	Eric的苹果可携式设备备份内,储存了枪的数张相片，是与网页thegunstorelasvegas.com有关，有多少张图片是存放于屏幕快照文件夹内？
	A.	2
	B.	3
√	C.	4
	D.	5
	E.	6

解析：在火眼数据分析软件中，基本信息－图片－屏幕快照下可见数张图片，预览图片后发现有四张图片与题目描述相符。

	103	根据该苹果可携式设备的备份所显示，下列哪三项有可能是Eric意图购买的枪械型号？
	i.	SPRINGFIELD √DS9 9MM
	ii	M4.223
	iii	MP45 M2.0
	iv	Springfield Armory SAINT AR-15 5.56/223 Carbine
	v	Springfield Armory SAINT AR-15 5.56/224 Carbine

	103	根据该苹果可携式设备的备份所显示，下列哪三项有可能是Eric意图购买的枪械型号？
	A.	i, ii, iii
	B.	iii, iv, v
√	C.	i, iii, iv
	D.	i, iii, v
	E.	全部皆是

解析：见上题图

	104	在Eric的苹果可携式设备的备份内,在其中一张相片中，显示一款枪价值是$949.9，你能找出该相片的MD5哈希值？
	A.	42b3e17a7d431f8c09ff319d970faae2

√

B.

63878942da949014adca2a1ce304caf0

C.

4caae44fbe76c22206dc986ac88b3006

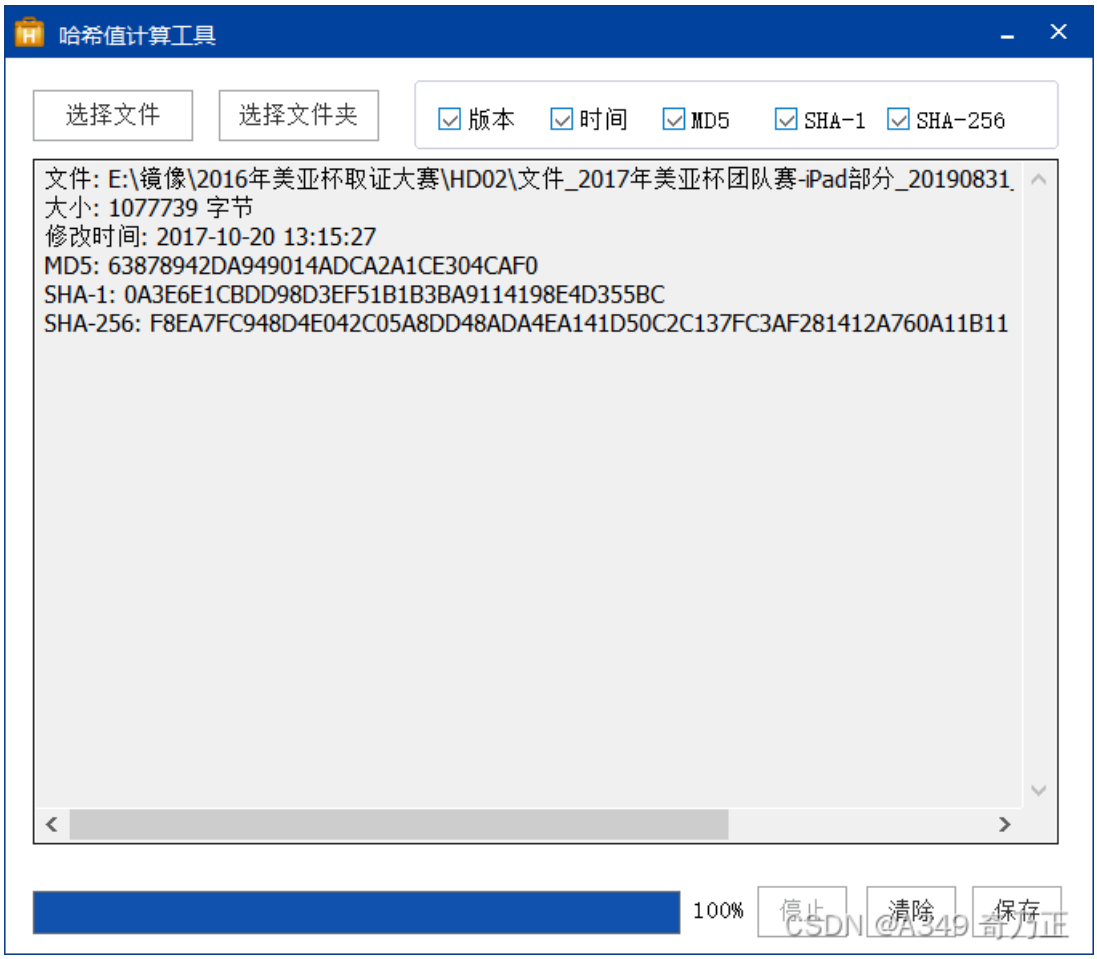
D.

4bc423d322bca4a1cf7b407ff31ad4cc

E.

82b53001f6ceb5181ffaef472097c24a

解析：第一步：找到图片位置，第二步：导出文件



	105	Eric的苹果可携式设备备份内，有多少相片与”深水战士”有关?
	A.	IMG_0006.JPG
	B.	IMG_0035.PNG

	105	Eric的苹果可携式设备备份内，有多少相片与”深水战士”有关？
√	C.	IMG_0060.PNG
	D.	IMG_0062.PNG
	E.	IMG_0072.JPG

解析：搜索文件名，按图找出相应图片