216SE PHASE TEST 2020/2021

This test will comprise of 2 elements: there will be a series of general digital forensics related questions followed by ones that will require usage of forensic software for examining evidence files to determine the answers.

DATE: 06/04/2021

SID Number: 9195071

READ THESE INSTRUCTIONS CAREFULLY AND FOLLOW THE STEPS OUTLINED.

This assessment is “guided book” you will receive every resource that you can use if you need to. Internet and course material should not be used.

You can make use all software on your system, but not the Internet, nor should you consult teaching material and classmates. Standard university assessment policies apply. All your working files should be created and located in a 216SE folder on your Desktop and should be removed once finished.

The test has **100 marks.**

READ THE QUESTIONS CAREFULLY AND ANSWER ACCORDINGLY.

TOTAL SCORE /100

A1: How might you capture temporary data on a running system? (2 marks)

a) Network sniffing
b) Application tracing
c) Live analysis
d) Offline analysis

a ( ) b ( ) c (X) d ( )

A2: Which term describes the continuity of evidence that makes it possible to account for all that has happened to evidence since it was collected? (2 marks)

a) Evidence log
b) Evidence access documentation
c) Chain of access
d) Chain of custody

a ( ) b (X) c ( ) d ( )

A3: What is file slack? (2 marks)

a) The space in a file left by deleting part of the file
b) The space between a start of sector mark and start-of-file
c) The space between start-of-file and the logical end-of-file
d) The space between the logical end-of file and the physical end-of-file

a ( ) b ( ) c ( ) d (X)

A4: Which term refers to computer criminals that are slightly more advanced than a newbie, but generally have limited experience with computers and networks? (2 marks)

a) Coders
b) Script kiddies
c) Cyberterrorists
d) Cyberpunks

a ( ) b (X) c ( ) d ( )

A5: Which of the following is not a drawback encountered with dead system forensics? (2 marks)

a) It leads to data corruption and system downtime.
b) Dead system forensic techniques are outdated.
c) Network-related data is not readily available.
d) Evidence degrades as time progresses.

a ( ) b ( ) c ( ) d (X)

A6: Where would you find information on how many times a user has logged on? (2 marks)

a) SECURITY registry file
b) NTUSER.dat
c) SAM registry file
d) SOFTWARE registry file
e) a (X) b ( ) c ( ) d ( )

Marks on page: /12

A7: In the UK there are some guidelines for handling and processing digital devices. What are these guidelines called? (2 marks)

a) ACPO Good Practice Guide for Computer-Based Electronic Evidence
b) ACPO guidelines on Digital Data
c) ACPO Good Practice Guide for Digital Evidence
d) The 4 Principles – ACPO Computer Data

a ( ) b ( ) c (X) d ( )

A8: Which term describes the data that provides information about a file? (2 marks)

a) Extended data
b) Schema
c) Metadata
d) File attributes

a ( ) b ( ) c (X) d ( )

A9: What type of volatile data has no forensic value? (2 marks)

(a) State of running processes
(b) State of network connections
(c) CPU Cache and register contents
(d) RAM contents

a ( ) b ( ) c (X) d ( )

A10: Describe what NTUSER.dat is and what it contains: (3 marks)

NTUSER.dat is a file unique to each user that contains specific settings for that user on the system.

A11: What is Locard's Exchange Principle? (3 marks)

Locard's exchange principle states that anything that touches something else will leave material on the other. In terms of forensics this means if we were to for example plug a device into a system there would be a transfer of material that could contaminate the digital evidence.

A12: Why is there a need for SSD Wear levelling? (2 marks)

Each read/write action on an SSD degrades the NAND chip slightly, in time completely degrading performance. As there are multiple NAND chips in an SSD, levelling this wear across all of them by evenly writing to all chips will increase the lifetime of the drive.

A13: Describe SSD TRIM: (3 marks)

____
____
____
____

A14: Name 5 rights that the GDPR provides for individuals: (5 marks)
The right to be informed, the right to be forgotten, the right to object, the right to access

Marks on page: /17

A15: In the event of a data breach involving personal data, companies must do what in terms of GDPR? (4 marks)

The company must inform the authorities within 24 hours, then inform customers within 48 hours.

A16: Describe SSD Forensic Data Corrosion: (3 marks)

____

____

____

____

A17: What is Phishing and what legislation deals with Phishing in the UK? (3 marks)

Phishing is the act of impersonating a figure of authority or someone with a close relation to the target. Then convincing the target to give up sensitive information or download a form of malware to extract information. The Computer Misuse Act 1990 section 3A could be used when prosecuting for phishing but the Fraud act 2006 would probably be better suited.

A18: Name 5 hives of Windows Registry and outline the data stored within them: (5 marks)

SAM – Group data

SOFTWARE – Software Settings

SYSTEM – System Data

SECURITY – Policy Data

NTUSER – User specific settings

A19: Which of the following regular expressions would find CV2 4NY and CV32 5EL but *NOT* PT26 8YX

(2 marks)

a) \<[\u\l][\u\l]?\d\d?\s\d[\u\l][\u\l]\>
b) \<[A-F][A-Z]\d\d\s[0-5][A-F][A-F]\>
c) \<[\u\l][\u\l]\d\d\s[0-5][\u\l][\u\l]\>
d) \<[\u\l][\u\l]?\d\d?\s[0-5][\u\l][\u\l]\>

a ( ) b ( ) c ( ) d (X)

Marks on page: /22

A20: Consider this scenario: **(**3 marks)

You are notified that a laptop belonging to a suspect has been located and there is evidence on the screen relating to methods of stealing credit cards. The officer seizing asks for advice as to how they can gain as much evidence as possible but has heard that there are guidelines as to what should be done in these circumstances. Which of the following statements **should be communicated** to the officer as advice on how the investigation should proceed?

(a) No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court. Take a photograph of the screen then remove the power cord and the battery from the laptop and recover it.

(b) This is a serious offence and, in these circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person should be guided by a competent person.

(c) An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. Make sure you keep all original notes and package the laptop.

(d) You should get an independent third party who should be able to examine those processes and achieve the same result.

a (X) b ( ) c ( ) d ( )

A20 (b) What section of the Computer Misuse Act deals with alteration of data? (1 marks)

3

A20 (c) What is the offence in question above? Detail its elements(Happenings and appropriate legislation): (5 marks)

____

____

____

____

____

____

____

____

Marks on page: /9

SECTION B Investigative skills **Marks Achievable in section: 40**

READ ALL INSTRICTIONS CAREFULLY

Download the PT.zip from aula. Extraction should reveal that you are given 6 evidence files to work on:

a) Application.evtx
b) Security.evtx
c) SAM,
d) Software
e) System
f) IDTheft 3.E01

And the supporting documentation: **Logs_IDs.pdf, Registry Guide.**

Once you have downloaded the evidence files listed above, you are to examine the evidence and answer specific questions concerning it. Work methodically and identify the items required. Rather than answering each question in consecutive order, you may wish to examine the evidence and conduct some searches to get a better understanding of the material.

Analyse the files attached. **It is up to you to know** which evidence item to find the required information in. In the case of **LOG FILES** your scope is restricted to entries happened on in the **evening, 4th of December 2017 between 18:00 and 22.00. Any entries falling into the time scope are valid.**

B1: Analysing the log files for the given scope above, answer the following: (6 Marks)

a) What applications have been installed?
- AccessData FTK Imager
- Autopsy
- Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.40649
- Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.40649
- Google Update Helper
- LCP 5.04
- Log Parser 2.2
- iTeleport Connect

b) What application at first failed to install?
- iTeleport Connect

c) Which account has been deleted and by which user?
mr.black was deleted by mr.pink

d) Which account has been disabled and by which user?
mr.green was disabled by mr.pink

e) Which account has been enabled and by which user?
mr.brown enabled 4 accounts between 18:00 and 22:00. These accounts are: mr.yellow, mr.blue, mr.black and mr.green. Later in the evening mr.green was then enabled again by mr.brown.

f) Which account name has been changed and by which user?
mr.green was changed to mr.violet by mr.brown

Marks on page: /6

B3: Analyse the registry files to find answers to the following questions:

a) What is the computer name? (1 Mark)
BROWN-DESK

b) Who is the Registered Owner? (1 Mark)
mr.brown

c) Which Operating System and exact version has been installed? (2 Marks)
Windows 10 pro release 1709

d) What is the Timezone in use on the machine? (1 Marks)
W. Europe Summer Time

e) Which model of network card has been installed and what is its GUID? (2 Marks)
Intel(R) 82574L Gigabit Network Connection
{BC764EC0-CD9E-4249-BC0C-43C8F944DDC2}

f) Has DHCP been enabled? (1 Marks)
Yes

g) What is the IP address of the machine? (1 Marks)
192.168.220.142

h) What is the IP address of the DHCP server? (1 Marks)
192.168.220.254

i) What are the subnet masks for all the networks found? (1 Marks)
255.255.255.0

Marks on page: /11

B2: Analysing IDTheft 3.E01 (12 Marks)

Sugested Tools: Autopsy ,Hxd and FTK Imager

Analysing IDTheft 3.E01 with the tools available answer the following questions:

1: What is the md5 verification hash of the e01 file?
5711420c1ce1fb6d9bc4666489554707

2: What OS has been Acquired?
Windows XP

3: When was the image Acquired?
21/12/2003 04:49:00

4: What is the main File System of the Image?
NTFS

5: What is the volume serial number? (5 Marks)
4294967280

6: List all the **non-built in** users on the image: (3 Marks)

- HelpAssistant
- SUPPORT_388945A0
- FTK User
- ASPNET
- PRTK
- Secret User

7: What is the MD5 and the file name of the last modified encrypted file?
(2 Marks)

File Name: This details ....doc
MD5: 3a97d29d7df99c16c59166d7fcbd2610

8: What is the email address of Linda Paws? (3 Marks)
LindaPaws@aol.com

THE END

Make sure you hit save, before you upload. Better, convert your answers (this document) into PDF and upload.

Marks on page: /13