No. of Printed Pages : 5 **MSEI-027**

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

June, 2012

00119

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

Note : ***Section A*** *- Answer* ***all*** *the objective type questions*

Section B *- Answer* ***all*** *the very short answer type questions.*

Section C *- Answer any 2 out of 3 short answer type questions.*

Section D *- Answer any 2 out of 3 long questions.*

SECTION-A
(Attempt all the questions)

1. FWD Stands for _____. **1**

(a) Finite Data Worm

(b) Fixed Worm Data

(c) Finite Wireless Data

(d) Fixed Wireless Data

2. A _____ attacker entices computer to log into a computer which is set up a AP (Access Point). Once this is done, the hacker connects to the real access point through another wireless cord offering a steady flow of traffic through the transparent hacking computer to a real Network. **1**

3. _____ stands for WEP. 1

4. DoS Stands for _____. 1

5. Internet protocol _____ is an attack in the internet provider where the attacker disguises himself or herself as another user by means of a false IP Network. 1

6. _____ is a form of fraud or cheating of another person's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. 1

7. SPF Stands for _____ and DAC Stands for _____. 1

8. Data theft is a growing problem primarily per petrated by office workers with access to technology such as desktop computers and hand held devices capable of storing digital information such as USB flash drivers, iPods, and even digital cameras. 1

(a) TRUE (b) FALSE

9. CSS Stands for Cascading Style Sheet. 1

(a) TRUE (b) FALSE

10. CFTT Stands for _____. 1

SECTION-B

(5 very short Answer type questions)
(Attempt all the questions)

11. Give difference between E-Mail Spoofing and E-Mail Bombing. **2**

12. What are the modes and characteristics of Ethical Hacking ? **2**

13. Define active and passive Reconnaissance in Hacking. **2**

14. Define Honeypots and IDS. **2**

15. What is the range of 802.20 ? Define i-Mode. **2**

SECTION-C

(Attempt 2 out of 3 short answer type Questions)

16. What is the prevention of unauthorized access or damage to computer using wireless network ? Define Radius. **5**

17. What are the three principal ways to secure a wireless network ? **5**

18. Define the following : **5**

(a) Identity Cloning and Concealment 2

(b) Criminal Identity theft

SECTION-D

(Attempt 2 out of 3 long Questions)

19. Explain three steps of investigating Nigerian fraud cases. What is data theft ? Define Ad-hoc network. **10**

20. Give Some techniques for obtaining and exploiting personal information for identity theft. Give any two differences between WEP and WPA. Define Trojan attack. **10**

21. Write short notes on the following : **5x2=10**

(a) Corder
(b) Worms
(c) Logic Bomb
(d) Spoofing
(e) Pornography

No. of Printed Pages : 5

MSEI-027

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

01272

December, 2012

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

*Note : Section 'A' - Answer **all** the objective type questions.*
*Section 'B' - Answer **all** the very short answer type questions.*
*Section 'C' - Answer **any two** questions out of **three** short answer type questions.*
*Section 'D' - Answer any **two** out of **three** long questions.*

SECTION - A

(Attempt all the questions)

1. WPA stands for _____. 1

   (a) Wi-Fi Protected Access
   (b) Wi-Fi Protected Antenna
   (c) Wi-Fi Protected Area
   (d) Wi-Fi Protected Architecture

2. http stands for "hyper text technical protocol". 1

   (a) True (b) False

3. _____ Stands for TCP. 1

4. DDoS Stands for _____. 1

5. The simulation is clearly related to a _____ attack as it targets the organization's equipment. 1

6. Area of investigation also need service of _____ to collect, analysis, and present computer based information so that it is suitable for use as evidence in court of lab. 1

7. GSM Stands for _____. 1

8. A _____ attacker entices computer to log into a computer, which is set up as a AP (Access Point). 1

9. In an _____, connections are made spontaneously such that a connection is made from the transmitting device to the receiver. 1

10. SSID Stands for _____. 1

SECTION - B

(5 very short answer type questions)

(Attempt all the questions)

11. Give any two difference between E-Mail Spamming and E-Mail Bombing. 2

OR

Define Data theft.

12. What is Electronic tempering ? 2

13. Define Identity theft. Define types of data theft. 2

14. Define Active and Passive Reconnaissance in Hacking. 2

15. Explain the use of IEEE 802.16. 2

SECTION - C

(Attempt 2 out of 3 short answer type questions)

16. Explain the advantages and disadvantages of software based firewall and hardware based firewall. 5

17. Define file Carving and Radius Server with examples. 5

18. Name two types of wireless securities. Explain the term logs and logging in collecting and Archiving. 5

SECTION - D

(Attempt 2 out of 3 long questions)

19. What is a log file analysis ? What is data theft ? Define Ad-hoc network. **10**

20. What is Intrusion Detection System ? How does it different from firewall ? Define IPS. **10**

21. Write a short note on the following : **5x2=10**

(a) Firewall

(b) Routers

(c) Logic bomb

(d) SNMP

(e) 802.11b, 802.11g wifi 2.

No. of Printed Page : 1

MSEI-027 (P)

POST GRADUATE DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Practical Examination

December, 2012

MSEI-027 (P) : DIGITAL FORENSICS

00532

Time : 3 hours *Maximum Marks : 100*

Note : (i) *Attempt* ***any two*** *questions out of* ***three*** *carrying* ***40*** *marks each.*

(ii) *Viva - voce carries* ***20*** *marks.*

1. Install the SMTP server by misguiding protocol. Explain the concept of Email bombing. How is it done on any email ID practically and generate the final report. **40**

2. Generate an anonymous email from hack@ignou.com and Drop the mail in any email ID. **40**

3. Spoof your IP and MAC address after spoofing. Verify whether your current system IP and MAC address is same as it was before ? **40**

No. of Printed Pages : 5

MSEI-027

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

00256

June, 2013

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

*Note : Section A - Answer **all** the objective type questions.*

*Section B - Answer **all** the very short answer type questions.*

*Section C - Answer **any two** questions out of three short answer type questions.*

*Section D - Answer any **two** questions out of three long questions.*

SECTION-A

Objective type questions

(Attempt *all* the questions)

1. FTC stands for _____. 1

   (a) Federal Trade Commission
   (b) Federal Trade Commissioner
   (c) Federal Trade Command
   (d) None of these

2. _____ is the world's first "smart phone" for web browsing and provides color and video over telephone sets. 1

3. A Multi Media Card (MMC) is a solid-state disk card with _____ number of pins connector. 1

4. MF, DF, EF are the types of file system for SIM. 1

(a) True (b) False

5. GSM stands for _____. 1

6. GPRS stands for _____. 1

(a) General Packet Radio Server

(b) General Packet Radio Service

(c) General Package Radio Server

(d) None of these

7. PUK stands for _____. 1

8. 802.119 used the data rate of _____ mbps. 1

9. Spam is the use of electronic messaging system to send unsolicited bulk messages indiscriminately. 1

(a) True (b) False

10. EDGE stands for Enhanced Data GSM Environment. 1

(a) True (b) False

SECTION-B

Very short type questions

(Attempt *all* the questions)

11. What is Spoofing ? 2

12. What is PDA Seizure ? 2

13. What is honeypotting ? 2

14. Define Bluetooth. 2

15. Write a short note on "Multi-Media Card". 2

SECTION-C

Short Answers type questions

(Attempt **2** out of **3** questions)

16. Give some examples of important computer related crimes in India. 5

17. How can one define digital investigations and digital evidence ? And when a complaint on information theft is received, how should one start investigation ? 5

18. What are the advantages of using wireless technology for computer network ? 5

SECTION-D

Long answers type questions

(Attempt **2** out of **3** questions)

19. Define i-mode. Explain the use of WPAN's. What is range of 802.20 ? List three classifications of wireless networks. 10

20. Explain "Log File Analysis". What is "File Carving" in Data Recovery ? What is Salvaging of Data ? 10

21. Write a short note on the following : 10

(a) SNMP

(b) Vital Information Resource under Siege

(c) Cyber Terrorism

(d) Root-Kits

(e) Cyber Bullying

No. of Printed Pages : 2

MSEI-027 (P)

00440

POST GRADUATE DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Practical Examination

June, 2013

MSEI-027 (P) : DIGITAL FORENSICS

Time : 3 hours *Maximum Marks : 100*

Note : (i) *Attempt 2 out of 3 questions. Each carries 40 marks.*

(ii) *Viva-voce carries 20 marks.*

1. By misguiding SMTP Protocol, explain the concept of E-mail Bombing and Generate the final report. 40

2. Generate the report on the basis of System Details/Logs. 40

   (a) Logs for USB Device

   (b) Logs for User Authentication

   (c) Logs for Application Errors

   (d) OS installation Date and Time

   (e) Screen Shot of System Up Time

   (f) OS product ID

   (g) Host Name

   (h) List of existing usernames on system

3. Do penetration testing and information gathering on http://sedulitygroups.org, try to find out the information as more as it can possible and generate the final report. 40

No. of Printed Pages : 2

MSEI-027 (P)

POST GRADUATE DIPLOMA IN INFORMATION SECURITY (PGDIS)

00271

Term-End Practical Examination

December, 2013

MSEI-027 (P) : DIGITAL FORENSICS

Time : 3 hours *Maximum Marks : 100*

Note : (i) *Attempt 2 out of 3 questions. Each carries 40 marks.*

(ii) *Viva-voce carries 20 marks.*

1. By misguiding SMTP and HTTP protocol, explain the concept of Fake mailing and phishing attacks and generate the final report. 40

2. Generate the report on the basis of System Details/ Logs. 40

   (a) Screen shot of system time up.

   (b) OS Product ID.

   (c) Logs for application errors.

   (d) List of existing user names on system.

   (e) Logs for USB Devices.

   (f) Logs for user Authentication.

   (g) Host name.

   (h) OS Installation Date and Time .

3. Do penetration Testing and Information gathering on Http:// Sedulity.in, try to find out the information as more as it can possible and generate the final report. 40

No. of Printed Pages : 3

MSEI-027

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

December, 2013

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

Note : ***Section A*** *- Answer* ***all*** *the objective type questions.*

Section B *- Answer* ***all*** *the very short answer type questions.*

Section C *- Answer* ***any two*** *out of* ***three*** *short answer type questions.*

Section D *- Answer* ***any two*** *out of* ***three*** *long questions.*

SECTION - A

Objective type questions. (Attempt all the questions) :

1. PDA stands for _____ . **1**

(a) Personal Digital Assistant

(b) Personal Digital Admin.

(c) Personal Digital Admission

(d) None of these

2. A Multi-Media Card (MMC) is a solid-state disk card with_____number of pins connector. **1**

3. _____ is the world first " smart phone" for web browsing provider color and video over telephone sets. 1

4. Full form of SM is _____ . 1

5. WAP stands for Wired Application Protocol. 1
(a) TRUE (b) FALSE

6. "PGP" stands for _____ . 1

7. "SSIDS" stands for _____ . 1

8. "TFTP" stnds for _____ . 1

9. EDGE stnds for Enhanced Data GSM Environment. 1
(a) TRUE (b) FALSE

10. _____ is the collection of infected computers or bots that have been taken over by hackers. 1

SECTION - B

Very short type questions. (Attempt all the questions)

11. What is WEP ? 2

12. Write a short note on types of Spam. 2

13. What is infrored ? 2

14. Write a short note on mobile forensics. 2

15. Write a short note on freezing the scene. 2

SECTION - C

Short answer type questions. (Attempt **2** out of **3** questions.)

16. What is Money Loundering ? What is Identity theft ? **5**

17. Explain only two tools used in "Forensics Examination of Mobile devices". **5**

18. Write a short note on data file integrity . Explain logical Backup and Bit Stream Imaging. **5**

SECTION - D

Long Answers type questions. (Attempt **2** out of **3** questions) :

19. Explain five stages of Ethical Hacking. **10**

20. What is the general process for conducting a digital investigation ? As on investigator what are different things that have to be determined / looked into for conducting an effective investigator ? **10**

21. Write a short note on the following : **5x2=10**

(a) Cyber - Stalking
(b) MAC
(c) Harassment
(d) SIM card Acquisition
(e) WIPS

No. of Printed Pages : 1

MSEI-027 (P)

POST GRADUATE DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Practical Examination

June, 2014

00407

MSEI-027 (P) : DIGITAL FORENSICS

Time : 3 hours *Maximum Marks : 100*

Note : *(i) Attempt any **two** questions out of three. Each question carries 40 marks.*

(ii) Viva-voce carries 20 marks.

1. By using any Data Acquisition/Recovery Tool, try to retrieve the details for the duration of last week, which are as follows : *40*

(a) DOC/DOCX files accessed

(b) E-mails received/sent

(c) Images downloaded from the Internet

(d) Exe files executed in the last week

2. Try to use some wireless sniffers and display the list of Access points available with their details like SSID, MAC Address, Distance and Channel ID running at any particular instance. *40*

3. Generate the list of the USB devices with their details applied on the existing Operating System for the duration of last one week. *40*

No. of Printed Pages : 3

MSEI-027

00982

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

June, 2014

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

*Note : Section A - Answer **all** the objective type questions.*

*Section B - Answer **all** the very short answer type questions.*

*Section C - Answer **any two** questions out of **three** short answer type questions.*

*Section D - Answer **any two** out of **three** long questions.*

SECTION - A

(Attempt **all** the questions)

1. A _____ occurs when the data from a suspect system is being copied without the assistance of the suspect operating system. 1

2. The full form of FIFO is _____ . 1

3. _____ is a collection of infected computers or bots that have been taken over by hackers and are used to perform malicious tasks or functions. 1

4. Regular auditing and accounting of your system is useful not only for detecting intruders but also as a form of _____ . 1

5. _____ is a windows - based acquisition and analysis tool that comes in both local and network - based versions. 1

6. _____ is any evidence presented by a person who was not a direct witness. 1

7. The _____ was established in 1995 to provide a forum for law enforcement agencies across the world to exchange information about computer forensics issues. 1

8. _____ is a digital object that contains reliable information that supports or refutes a hypothesis. 1

9. _____ is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. 1

10. _____ is the programming instructions that are compiled into the executable files that are sold by software development companies. 1

SECTION - B

(5 very short answer type questions)

(Attempt **all** the questions)

11. What is electronic tempering ? 2

12. What are the techniques for obtaining and exploiting personal information for identity theft ? 2

13. Explain the types of Spam. 2

14. What is exculpatory evidence ? 2

15. What are the two basic forms of collection ? 2

SECTION - C

(Attempt **2** out of **3** short answer type questions)

16. Write short notes on : **2.5x2=5**

(a) Cyber terrorism

(b) Identity theft

17. Explain the major characteristics of financial crimes. **5**

18. Electronic crime is difficult to investigate and prosecute. Elaborate this statement. **5**

SECTION - D

(Attempt **2** out of **3** long questions)

19. What are the issues involved with detection of cyber crimes in India ? **10**

20. You are working as a investigator for looking over the intellectual properties policies of the company "XYZ Ltd" and to check for the violations, if any. How you will plan your investigation and what are the main questions which you will ask the company and its employees ? **10**

21. Forensic analysis of digital evidence depends on the case context and largely relies on the knowledge, experience, expertise, thoroughness and in some cases the curiosity of the practioner performing the work. Do you agree ? Explain the underlying process of forensic analysis in detail. **10**

No. of Printed Pages : 1

MSEI-027 (P)

POST GRADUATE DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Practical Examination

00014

December, 2014

MSEI-027 (P) : DIGITAL FORENSICS

Time : 3 hours *Maximum Marks : 100*

Note : *(i) Attempt any 2 questions out of 3 carrying 40 marks each.*

(ii) Viva-voce carries 20 marks.

1. Apply the forensics tools on the Pen-Drive / Mobile Memory Card and do the Data Acquisition / Recovery of the following : *40*

(a) DOC/DOCX files

(b) MP3/MPEG files

(c) JPG/JPEG/GIF files

(d) 3GP/AVI files

2. Calculate the MD5 hash value for any file or folder and copy the file or folder to some other location on the network and then recalculate the MD5 and compare whether the value of MD5 is the same or different. Display the list of the DOC files accessed from the Pen Drive from the system. *40*

3. Apply some wireless sniffer tool and display the list of Access Points available with their details like SSID, MAC Address, Distance and Channel ID running at any particular instance. *40*

No. of Printed Pages : 4

MSEI-027

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

00904

December, 2014

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

Note :

*Section A – Answer **all** the objective type questions.*

*Section B – Answer **all** the very short answer type questions.*

*Section C – Answer any **two** questions out of three short answer type questions.*

*Section D – Answer any **two** questions out of three long answer type questions.*

SECTION A

Attempt all the following questions. *10×1=10*

1. _____ is one where the suspect operating system is still running and being used to copy data. *1*

2. _____ is the full form of BIOS. *1*

3. An _____ is a form of Internet text messaging or synchronous conferencing. *1*

4. _____ is "an information resource whose value lies in unauthorized or illicit use of that resource". *1*

5. The _____ is an online publication devoted to discussions of the theory and practice of handling digital evidence. *1*

6. Whenever a system is compromised, there is almost always something left behind by the attacker be it code fragments, trojaned programs, running processes, or sniffer log files. These are known as _____ . *1*

7. The _____ is a non-profit organisation that is dedicated to educating law enforcement professionals in the area of computer forensics. *1*

8. _____ is the intentional or unintentional use of a portable USB mass storage device to illicitly download confidential data from a network endpoint. *1*

9. A _____ is a process where we develop and test hypotheses that answer questions about digital events. *1*

10. The field of _____ involves identifying, extracting, documenting and preserving information that is stored or transmitted in electronic or magnetic form. *1*

SECTION B

Answer all 5 very short answer type questions. *5×2=10*

11. Define types of data theft. *2*

12. Why is spam so prevalent on the Internet ? *2*

13. Which one is more ideal – dead analysis or live analysis and why ? *2*

14. What is volatile evidence ? *2*

15. What are the three major phases of Digital forensics ? *2*

SECTION C

Answer any 2 questions out of 3 short answer type questions. *2×5=10*

16. Write short notes on the following : $2\frac{1}{2} \times 2 = 5$

(a) Cyber bullying

(b) Data theft

17. Explain the major characteristics of white collar economic crimes. *5*

18. Explain the background of botnets. *5*

SECTION D

Answer any 2 questions out of 3 long answer type questions. *2×10=20*

19. Cyber crime is a rapidly growing field and problem area for law enforcing agencies. Do you agree ? Explain in detail. *10*

20. What are the items that need to be considered for conducting an effective investigation for cyber crime ? *10*

21. Explain the five rules of collecting electronic evidence in detail. *10*

No. of Printed Page : 1

MSEI-027 (P)

00971

POST GRADUATE DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Practical Examination

June, 2015

MSEI-027 (P) : DIGITAL FORENSICS

Time : 3 hours *Maximum Marks : 100*

Note : *(i) Attempt* **2** *out of* **3** *questions. Each carries* **40** *marks.*

(ii) Viva-voce carries **20** *Marks.*

1. How to identify fake mail using header information of an email ? Send a mail using fake-mailer and also from a genuine email-id and show the header analysis of email. **40**

2. How to retrieve the deleted data from the drive ? Show the steps involve in it. **40**

3. Analyze audit trails of Windows to find out information about the following terms : **40**

(a) Logic bomb

(b) Vulnerability

(c) Exploit

(d) Back door entry and trapdoor

No. of Printed Pages : 4

MSEI-027

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

00951

Term-End Examination

June, 2015

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

Note : (i) ***Section 'A'*** *- answer* ***all*** *the objective type questions.*

(ii) ***Section 'B'*** *- answer* ***all*** *the very short answer type questions.*

(iii) ***Section 'C'*** *- answer* ***any two*** *questions out of* ***three*** *short answer questions.*

(iv) ***Section 'D'*** *- answer* ***any two*** *out of* ***three*** *long questions.*

SECTION - A

(Attempt **all** the questions)

1. Which Intrusion Detection System (IDS) usually provide the most false alarm due to unpredictable behaviors of users and networks ? 1

   (a) Network based IDS system (NIDS)
   (b) Host based IDS system (HIDS)
   (c) Anomaly Detection
   (d) Signature recognition

2. _____ refers to the unauthorized entry into a computer system. 1

3. _____ is the science of acquiring, preserving, retrieving and presenting data that has been processed electronically and stored on computer media. 1

4. The first step in a digital Forensics process is _____. 1

5. GSM stands for _____. 1

6. Ubuntu is a(n) _____. 1

7. _____ is the use of the internet or the other electronic means to stalk or harass an individual, a group of individual, or an organization. 1

8. The name of website containing periodic posts_____. 1

9. When examining hard disk without a write-blocker, you should not start windows because windows will write data to the : 1

(a) Recycle Bin
(b) Case files
(c) BIOS
(d) MSDOS. sys

10. When performing a forensic analysis, what device is used to prevent the system from recording data on an evidence disk ? 1

(a) Write-blocker
(b) Protocal Analyzer
(c) Firewall
(d) Disk Editor

SECTION - B

(5 very short answer questions)
(Attempt **all** questions)

11. What is electronic tempering ? **2**

12. Define Active and Passive Reconnaissance in Hacking. **2**

13. Differentiate "copy of the drive"and "imaging of the drive". **2**

14. What is firewall ? **2**

15. What is cloud forensic ? **2**

SECTION - C

(Attempt **2** out of **3** short answer questions)

16. What are some initial assessment you should make for a computing investigation ? **5**

17. Explain Daubert Guideline. Why these guidelines helpful in the digital forensic investigation. **5**

18. What is IMEI ? Why it is used in mobile phone devices ? How it is helpful in forensic investigation ? **5**

SECTION - D

(Attempt **2** out of **3** long questions)

19. Discuss the levels of analysis for data acquisition from mobiles phones. **10**

20. How digital evidence is processed ? What are the steps involved in Evidence Acquisition ? Explain with the help of hypothetical case. **10**

21. Write short notes on the following : **5x2=10**

(a) Hacking

(b) Cloning in forensic analysis

(c) Digital Evidence

(d) Admissible Evidence

(e) Logic Bomb

No. of Printed Page : **1**

MSEI-027 (P)

00469

POST GRADUATE DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Practical Examination

December, 2015

MSEI-027 (P) : DIGITAL FORENSICS

Time : 3 hours *Maximum Marks : 100*

Note : *(i) Attempt* **2** *out of* **3** *questions. Each carries* **40** *marks.*

(ii) Viva-voce carries ***20*** *Marks.*

1. Target any domain e.g. www.yahoo.com to gather following information : **40**

(a) Daily page views.
(b) Source of maximum traffic.
(c) Most popular page of website.
(d) WHO's information
(e) Rank of the website
(f) Security loopholes if any.

2. How to identify phishing website ? Explain the concept of phishing attack and generate the final report. **40**

3. How to find IMEI number of the mobile phone ? How this number is useful in the forensic investigation ? Generate an audit report for the Smart Phone. **40**

No. of Printed Pages : 4

MSEI-027

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

00702

Term-End Examination

December, 2015

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

Note : *(i)* ***Section 'A'*** *- Answer* ***all*** *the objective questions.*

(ii) ***Section 'B'*** *- Answer* ***all*** *the very short answer questions.*

(iii) ***Section 'C'*** *- Answer* ***any two*** *questions out of* ***three*** *short answer questions.*

(iv) ***Section 'D'*** *- Answer* ***any two*** *out of* ***three*** *long questions.*

SECTION - A

(Attempt **all** the questions)

1. In General, _____ involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve data. **1**

2. In microsoft file structure, sectors are rounded together to form _____. **1**

3. The _____ refers to handing over the results of private investigations to the authorities because of indications of criminal activity. **1**

4. _____ field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death. 1

5. In a computer forensic investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court ? 1

   (a) Rules of evidence.

   (b) Law of probability.

   (c) Chain of custody.

   (d) Policy of separation.

6. When examining a file with a Hex Editor, what space does the file header occupy ? 1

   (a) The last several bytes of the file.

   (b) The first several bytes of the file.

   (c) None, file header are contained in the FAT.

   (d) One byte at the beginning of the file.

7. What does the acronym POST mean as it relates to a Pc ? 1

   (a) Primary Operations Short Test.

   (b) Power On Self Test.

   (c) Pre Operational Situation Test.

   (d) Primary Operating System Test.

8. To preserve digital evidence, an investigator should _____. 1

(a) Make two copies of each evidence item using a single imaging tool.

(b) Make a single copy of each evidence item using an approved imaging tool.

(c) Make two copies of each evidence item using different imaging tools.

(d) Only store the original evidence item.

9. http stands for "hyper text transfer protocol". 1

(a) True (b) False

10. DDoS stands for _____. 1

SECTION - B

(5 very short answer questions)

(Attempt **all** questions)

11. What is cloning in forensic analysis ? 2

12. What is admissible evidence ? 2

13. Differentiate "copy of the drive" and "imaging of the drive" ? 2

14. What is Logic Bomb ? 2

15. What is cloud forensic ? 2

SECTION - C

(Attempt **2** out of **3** short answer type questions) **5**

16. Explain the principles of Computer - Based Evidence.

17. What are legal issues involved in seizure of the computer equipment ? **5**

18. Explain any digital forensic investigation model. **5**

SECTION - D

(Attempt **2** out of **3** long questions)

19. Explain the classification of CFCC (Cyber Frand and Cyber Crime). What are the pre-search preparations required for the forensic investigation case ? **10**

20. What is Intrusion Detection System ? How it is different from firewall ? **10**

21. Write a short note on the following : **5x2=10**

(a) Firewall.

(b) Hacking.

(c) Electronic tempering.

(d) Logic bomb.

(e) IEEE 802.16.

No. of Printed Pages : **1**

MSEI-027 (P)

00320

POST GRADUATE DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Practical Examination

June, 2016

MSEI-027 (P) : DIGITAL FORENSICS

Time : 3 hours *Maximum Marks : 100*

Note : *(i) Attempt* **2** *out of* **3** *questions. Each question carries* **40** *marks.*

(ii) Viva-voce carries **20** *Marks.*

1. Apply the forensic tools on the Pen-Drive/Mobile Memory Card and do Data Acquisition/Recovery of the following : **40**

(a) DOC/DOCX files

(b) MP3/MPEG files

(c) JPG/JPEG/GIF files

(d) 3GP/AVI files

2. Try to use some wireless snitlers and display the list of Access points available with their details like SSID, MAC address, Distance and Channel ID running at any particular instance. **40**

3. Generate the list of the USB devices with their details applied on the existing Operating System for the duration of last one week. **40**

No. of Printed Pages : **4**

MSEI-027

00801

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

June, 2016

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

Note : *(i)* ***Section A*** *- Answer* ***all*** *the objective type questions.*

(ii) ***Section B*** *- Answer* ***all*** *the very short answer type questions.*

(iii) ***Section C*** *- Answer* ***any two*** *out of* ***three*** *short answer type questions.*

(iv) ***Section D*** *- Answer* ***any two*** *out of* ***three*** *long answer type questions.*

SECTION - A

(Attempt **all** the questions.)

1. FTC stands for _____. **1**

(a) Federal Trade Commission

(b) Federal Trade Commissioner

(c) Federal Trade Command

(d) None of these

2. RSA is _____ key cryptosystem. **1**

3. DDOS stands for _____. **1**

4. A _____ attacker entices computer to log into a computer, which is set up as an AP (Access Point). 1

5. _____ is a collection of infected computers or bots that have been taken over by hackers and are used to perform malicious tasks or functions. 1

6. _____ is a digital object that contains reliable information that supports or refutes a hypothesis. 1

7. _____ is a computer program that can copy itself and infect a computer. 1

8. An _____ is a form of internet text messaging or synchronous conferencing. 1

9. WAP stands for Wired Application Protocol : 1

   (a) True

   (b) False

10. "PGP" stands for _____. 1

SECTION - B

Very short type of questions.

(Attempt **all** the questions.)

11. What is Spoofing ? **2**

12. What is 'Identity theft' ? Define types of data theft. **2**

13. What is exculpatory evidence ? **2**

14. Differentiate "copy of the drive" and "imaging of the drive". **2**

15. What are three major phases of Digital Forensics ? **2**

SECTION - C

(Attempt **2** out of **3** short type questions.)

16. What is Money laundering ? **5**

17. Explain the advantages and disadvantages of software based firewall and hardware based firewall. **5**

18. What are some initial assessment you should make for a computing investigation ? **5**

SECTION - D

(Attempt **2** out of **3** long questions.)

19. Explain "Log File Analysis". What is "File Carving" in Data recovery ? What is salvaging of data ? **10**

20. What is Intrusion Detection System ? How does it different from firewall ? Define IPS. **10**

21. Write a short note on the following : **10**

(a) Cyber bullying

(b) SIM Card Acquisition

(c) Cyber Terrorism

(d) Admissible Evidence

(e) Logic Bomb

No. of Printed Pages : **4**

MSEI-027

00022

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

December, 2016

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

Note : *(i)* ***Section A*** *- Answer* ***all*** *the objective type questions.*

(ii) ***Section B*** *- Answer* ***all*** *the very short answer type questions.*

(iii) ***Section C*** *- Answer* ***any two*** *out of* ***three*** *short answer type questions.*

(iv) ***Section D*** *- Answer* ***any two*** *out of* ***three*** *long answer type questions.*

SECTION - A

(Attempt **all** the questions.)

1. PDA stands for : **1**

(a) Personal Digital Assistant

(b) Personal Digital Admin.

(c) Personal Digital Admission

(d) None of these

2. A Multi-Media Card (MMC) is a solid state disk card with _____ number of pins connector. **1**

3. Class 1 Bluetooth devices have the range of _____ metres. **1**

4. GPRS stands for : 1

(a) General Packet Radio Server
(b) General Packet Radio Service
(c) General Package Radio Server
(d) None of these

5. _____ is the collection of infected computers or bots that have been taken over by hackers. 1

6. EDGE stands for Enhanced Data Rate for GSM Evolution. 1

(a) True (b) False

7. The full form of FIFO is _____. 1

8. _____ is the full form of BIOS. 1

9. "SSIDS" stands for _____. 1

10. "TFTP" stands for _____. 1

SECTION - B

(5 very short answer type questions)

(Attempt **all** the questions)

11. What is volatile evidence ? 2

12. Write a short note on freezing the scene. 2

13. What is honey potting ? 2

14. Give any two differences between E-mail Spamming and E-mail Bombing. 2

15. Which one is more ideal-dead analysis or live analysis and why ? 2

SECTION - C

(Attempt 2 out of 3 short answer type questions)

16. What are the legal issues involved in seizure of the computer equipment ? Explain the principal of Computer - Based Evidence. 5

17. Explain the major characteristics of financial crimes. 5

18. Explain any two tools used in "Forensics Examination of Mobile Devices". 5

SECTION - D

(Attempt 2 out of 3 long questions)

19. What is Digitized document forensic ? In computer investigation how the printout can be investigated and how the investigator come to know about the printer and from which the print had been taken. 10

20. What are the items that need to be considered for conducting an effective investigation for cyber crime ? 10

21. Write a short note on the following : 10

(a) SNMP

(b) Root - kits

(c) Data theft

(d) Cloning in forensic analysis

No. of Printed Pages : **1**

MSEI-027 (P)

00162

POST GRADUATE DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Practical Examination

December, 2016

MSEI-027 (P) : DIGITAL FORENSICS

Time : 3 hours *Maximum Marks : 100*

Note : (i) *Attempt* **2** *out of* **3** *question. Each question carries* **40** *marks.*

(ii) *Viva-voce carries* **20** *Marks.*

1. By misguiding SMTP Protocol, explain the concept of E-mail Bombing and generate the final report. **40**

2. Generate the report on the basis of System Details/Logs. **40**

(a) Screen shot of system time up.
(b) OS Product ID.
(c) Logs for application errors.
(d) List of existing user names on system
(e) Logs for USB Devices
(f) Logs for user Authentication
(g) Host name
(h) OS installation Date and Time

3. How to retrieve the deleted data from the drive ? Show the steps involve in it. **40**

No. of Printed Pages : 3

MSEI-027

00308

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

June, 2017

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

Note : *(i)* ***Section A*** *- Answer* ***all*** *the objective questions.*

(ii) ***Section B*** *- Answer* ***all*** *the very short answer questions.*

(iii) ***Section C*** *- Answer* ***any two*** *questions out of three short answer type questions.*

(iv) ***Section D*** *- Answer* ***any two*** *out of three long answer type questions.*

SECTION - A

(Attempt all the questions)

1. RAID stands for _____. 1

2. SNMP stands for _____. 1

3. SSID stands for _____. 1

4. IRC stands for _____. 1

5. TCP/IP Protocol used behind ping command (True/False) 1

6. AAA Protocol/Service in RADIUS stands for _____. 1

7. An Indian Act called as _____ to handle cyber frauds. 1

8. DD command in Linux used for Wireless Password recovery. (True/False) 1

9. IMAP stands for _____. 1

10. WPA stands for _____. 1

SECTION - B

(5 very short answer questions)

(Attempt **all** questions)

11. What is file Carving and Blue-snarfing ? 2

12. Explain salvaging of data. 2

13. What is log Analysis ? Explain with example. 2

14. What is Seizure ? Explain. 2

15. What is CDR ? How it helps for investigation ? 2

SECTION - C

(Attempt **2** out of **3** short answer type questions)

16. What is the difference between Firewall, IDS and IPS ? 5

17. Difference between Passive and Active Reconnaissance in Hacking. 5

18. What is Money Laundering and Phishing ? 5

SECTION - D

(Attempt **2** out of **3** long answer type questions)

19. What is the difference between WIFI and WI MAX, specify their standards, technical characteristics and security Policies ? **10**

20. What is the Procedure of RAM forensics, Hard disk forensics and Mobile Forensics ? **10**

21. Explain the following : **2x5**

(a) Human Trafficking
(b) Cyber Stalking
(c) TKIP
(d) SIM card Analysis
(e) Data Recovery

No. of Printed Pages : 2

MSEI-027 (P)

00313

POST GRADUATE DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Practical Examination

June, 2017

MSEI-027 (P) : DIGITAL FORENSICS

Time : 3 hours *Maximum Marks : 100*

Note : (i) Attempt 2 out of 3 questions. Each question carries 40 marks.

(ii) Viva-voce carries 20 Marks.

---

1. Select a Pen drive/Removable External drive, find all Artifacts from the removable drive, also create image of the same Pen drive and calculate its MDS and SHAI Hash value. **40**

2. Identify Network Forensics details as given below using any Sniffer like Wireshark etc. **40**

   (a) List the real time IP address and their MAC address connected to the host.

   (b) List the http from method content requested by the specific IP.

   (c) List the IP address sending the Packets to post 25 or 80 as a source or destination post.

   (d) List of the Protocols like ICMP, ARP, and DNS Packets only.

3. Take any Smart Phone and find details given below. **40**

(a) Technical Configuration of the Mobile Phone.

(b) Find details of WiFi interface card like IP address, MAC address SSID details and signal strength etc.

(c) Analysis list of Apps installed and running on the phone.

(d) List real time IP address and their ports communicating to the phone.

No. of Printed Pages : 3

MSEI-027

00793

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

December, 2017

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

Note : *(i)* ***Section 'A'** - Answer **all** the objective questions.*

(ii) ***Section 'B'** - Answer **all** the very short answer questions.*

(iii) ***Section 'C'** - Answer **any two** questions out of **three** short answer type questions.*

(iv) ***Section 'D'** - Answer **any two** out of three long answer type questions.*

SECTION - A

(Attempt all the questions)

1. SHA stands for _____. 1

2. IMEI stands for _____. 1

3. PUK stands for _____. 1

4. GPRS stands for _____. 1

5. UDP Protocol also use 3 ways Handshake for connection establishment. (True/False) 1

6. What is the latest file system used in LINUX 64 bit OS ? 1

7. MAC address defined in NIC Chipset. (**True/False**) 1

8. _____ Command, commonly use in Linux to create hard disk image. 1

9. ICMP Protocol use behind _____ Command. 1

10. _____ bits size for IPV6 Protocol. 1

SECTION - B

(5 Very short answer questions)

(Attempt all questions)

11. Define Cyber Bullying and Cyber Terrorism. 2

12. Define Botnets and E-mail Spams. 2

13. Define Boot Loaders with examples. 2

14. Explain the image file format. Explain embedded image. 2

15. Explain Ad hoc mode of operation. 2

SECTION - C

(Attempt 2 out of 3 short answer type questions)

16. What are the Artifacts of Cyber forensics ? What are the Artifacts collection steps generally used ? 5

17. What is the difference between Logical Data Acquisition and Physical Data Acquisition ? 5

18. What is the process of LOG File Analysis ? How to Reconstruct Deleted Files ? 5

SECTION - D

(Attempt **2** out of **3** long answer type questions)

19. What is the difference between WiFi 802.11b, 802.11g and 802.11n series ? **10**

20. Explain any 5 Email and IRC related Crimes. **10**

21. What do you mean by steganography ? Explain in detail. What are Symmetric and Asymmetric types ? **10**

No. of Printed Pages : **2**

MSEI-027 (P)

0413

POST GRADUATE DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Practical Examination

December, 2017

MSEI-027 (P) : DIGITAL FORENSICS

Time : 3 hours *Maximum Marks : 100*

Note : (i) Attempt 2 out of 3 questions. Each question carries 40 marks.

(ii) Viva-voce carries 20 Marks.

1. Select an image, find Artifacts of the image, apply steganography on the image and generate the new image. By using any reverse engineering or forensics tools, find the hidden file details from the steganographic image. 40

2. Identify Networks Forensics details as given below using any Sniffer like Wireshark etc. 40

   (a) Shows all TCP Packets that contain the word "Facebook".

   (b) Displays all HTTP responses that were sent more than 2 seconds after the request.

   (c) Sets a filter for any packet with X.X.X.X as the source or dest IP.

   (d) List of the protocols like ICMP, ARP, SMTP and DNS Packets only.

3. Take a Removable External drive or pen drive. Find all Artifacts from the removable drive, delete some files and than try to recover those files and calculate its MD5 and SHA1 Hash Values. **40**

No. of Printed Pages : **4**

MSEI-027

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

01423

Term-End Examination

June, 2018

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

Note : *(i)* ***Section A*** *- Answer* ***all*** *the objective type questions.*

(ii) ***Section B*** *- Answer* ***all*** *the very short answer type questions.*

(iii) ***Section C*** *- Answer any two out of three short answer type questions.*

(iv) ***Section D*** *- Answer any two out of three long answer type questions.*

SECTION - A

(Attempt **all** the questions)

1. What is the most significant legal issue in computer forensic ? **1**

(a) Preserving Evidence
(b) Seizing Evidence
(c) Admissibility of Evidence
(d) Discovery of Evidence

2. When a file is deleted ? **1**

(a) The file remains intact.
(b) The FAT entry for the file is zeroed out so it shows that the area is available for use by a new file.
(c) The first character of the directory entry file name is changed to a special character.
(d) All of the above.

3. Which of the following is not a property of computer evidence ? 1
   (a) Authentic and Accurate
   (b) Complete and convincing
   (c) Duplicated and preserved
   (d) Conform and Human Readable

4. _____ is the science of hiding messages in messages. 1
   (a) Scanning
   (b) Spoofing
   (c) Steganography
   (d) None

5. When shutting down a computer, what information typically lost ? 1
   (a) Data in RAM memory
   (b) Running Processes
   (c) Current network connections
   (d) All of the above

6. USB drives use _____. 1
   (a) RAM memory
   (b) Cache memory
   (c) Flash memory
   (d) None of the above

7. As a good forensic practice, why would it be a good idea to wipe a forensic drive before using it ? 1
   (a) Chain of custody
   (b) No need to wipe
   (c) Different file and operating system
   (d) Cross-contamination

8. Which of the following is an example of input device ? 1
   (a) Scanner
   (b) Speaker
   (c) CD
   (d) Printer

9. The operating system is the most common type of _____ software. 1
   (a) Communication
   (b) Application
   (c) System
   (d) Word-processing software

10. _____ are computers that excel at executing many different computer programs at the same time. 1

SECTION - B

(5 Very short answer type questions)
(Attempt **all** questions)

11. What are the techniques for obtaining and exploiting personal information for identity theft ? 2

12. What are the three major phases of Digital forensic ? 2

13. Differentiate "copy of the drive" and "imaging of the drive". 2

14. Define Active and Passive Reconnaissance in Hacking. 2

15. Define windows registry. Why it is important in forensic ? 2

SECTION - C

(Attempt **2** out of **3** short answer type questions)

16. What are some initial assessment you should make for a computing investigation ? **5**

17. How forensic analysis is done on windows and mobile devices ? **5**

18. What is data acquisition and duplication ? Give a brief description of data acquisition tools. **5**

SECTION - D

(Attempt **2** out of **3** long answer type questions)

19. Explain the classification of CFCC (Cyber Fraud and Cyber Crime). What are the pre-search preparation required for the forensic investigation case ? **10**

20. What are the counterfeit documents ? What are steps involved in detectional counterfeit documents ? Give a brief note on the duties performed by the examiner. Also discuss the elements of a forensic report. **10**

21. Write short notes on the following : (**any four**) **2.5x4=10**

(a) Cyber terrorism
(b) Forensic Auditing
(c) Logic bomb
(d) Cyber bullying
(e) Identity theft

No. of Printed Pages : 1

MSEI-027 (P)

00585

POST GRADUATE DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Practical Examination

June, 2018

MSEI-027 (P) : DIGITAL FORENSICS

Time : 3 hours *Maximum Marks : 100*

Note : *(i) Attempt 2 out of 3 questions. Each carries 40 marks.*
(ii) Viva-voce carries 20 marks.

1. How to identify fake mail using header information of an email ? Send a mail using fake-mailer and also from a genuine email-id and show the header analysis of email. **40**

2. How to retrieve the deleted data from the drive ? Show the steps involve in it. **40**

3. Do penetration testing and Information gathering on http://www.rediff.com, try to find out the information as more as it can possible and generate the final report. **40**

No. of Printed Pages : **4**

MSEI-027

01312

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

December, 2018

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

Note : *(i)* ***Section A*** *- Answer* ***all*** *the objective type questions.*

(ii) ***Section B*** *- Answer* ***all*** *the very short answer type questions.*

(iii) ***Section C*** *- Answer* ***any two*** *out of* ***three*** *short answer type questions.*

(iv) ***Section D*** *- Answer* ***any two*** *out of* ***three*** *long answer type questions.*

SECTION - A

(Attempt **all** the questions)

1. _____ is the full form of BIOS. 1

2. Computer forensics involves all of the following started activities except : 1
   (a) manipulation of computer data.
   (b) extraction of computer data.
   (c) interpretation of computer data.
   (d) preservation of computer data.

3. A drive is prepared in three processes. This processes include all of the following except : 1
   (a) high-level formatting
   (b) low-level formatting
   (c) formatting
   (d) partitioning

4. All of the following are examples of real security and privacy risks except : 1

(a) hackers (b) spam
(c) viruses (d) identity theft

5. Which of the following is NOT one of the four major data processing functions of a computer ? 1

(a) gathering data
(b) processing data into information
(c) analyzing the data or information
(d) storing the data or information

6. Computer gather data, which means that they allow users to _____ data. 1

7. As a good forensic practice, why would it be a good idea to wipe a forensic drive before using it ? 1

(a) Chain of custody
(b) No need to wipe
(c) Different file and Operating systems
(d) Cross-contamination

8. Which duplication method produces an exact replica of the original drive ? 1

(a) Bit-Stream Copy (b) Image Copy
(c) Mirror Copy (d) Drive Image

9. The binary language consists of two digits : _____ and _____. 1

10. Output devices store instructions or data that the CPU processes. 1

(a) True (b) False

SECTION - B

(5 very short answer type questions)

(Attempt **all** questions)

11. Once you format your hard drive, does it erase everything or can information still be retrieved. 2

12. Explain the difference between "live acquistion"and "post mortem acquisition". 2

13. What is CoC (Chain of Custody) and why is it important for evidence integrity ? 2

14. What are the different formats for digital evidence ? 2

15. What are the components of disk drives ? 2

SECTION - C

(Attempt 2 out of 3 Short answer type questions)

16. How can deleted data be retrieved from a PC ? How it is possible to know what Internet sites have been visited ? 5

17. State and explain the general tasks that the investigators perform when working with digital evidence. 5

18. Describe procedures for acquiring data from cell phones and mobile devices. 5

SECTION - D

(Attempt **2** out of **3** long questions)

19. What are the items that need to be considered for conducting an effective investigation for Cyber Crime ? **10**

20. What is Intrusion Detection System ? How it is different from fire wall ? **10**

21. Write Short note on the following : **2.5x4=10**

(a) Logic Bomb
(b) Admissible Evidence
(c) Roof-kits
(d) Hacking

No. of Printed Pages : 1

MSEI-027 (P)

00182

POST GRADUATE DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Practical Examination

December, 2018

MSEI-027 (P) : DIGITAL FORENSICS

Time : 3 hours *Maximum Marks : 100*

Note : (i) Attempt 2 out of 3 questions. Each question carries 40 marks.

(ii) Viva-voce carries 20 marks.

1. Try to use some wireless sniffers and display the list of Access points available with their details like SSID, MAC Address , Distance and Channel ID running at any particular instance. **40**

2. Generate the list of the USB devices with their details applied on the existing Operating System for the duration of last one week. **40**

3. By misguiding SMTP and HTTP protocol, explain the concept of Fake mailing and phishing attacks and generate the final report. **40**

No. of Printed Pages : 4

MSEI-027

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

01254

June, 2019

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

Note :

*Section A – Answer **all** the objective type questions.*

*Section B – Answer **all** the very short answer type questions.*

*Section C – Answer any **two** questions out of three short answer type questions.*

*Section D – Answer any **two** questions out of three long answer type questions.*

SECTION A

*Attempt **all** the questions.*

1. _____ refers to the unauthorized entry into a computer system. *1*

2. The first step in a digital forensic process is _____. *1*

3. The name of website containing periodic posts is _____. *1*

4. _____ is the collection of infected computers or bots that have been taken over by hackers. *1*

5. A _____ attacker entices computer to log into a computer, which is set up as an AP (Access Point). *1*

6. SSID stands for _____. *1*

7. SNMP stands for _____. *1*

8. IMAP stands for _____. *1*

9. In Microsoft file structure, sectors are rounded together to form _____. *1*

10. _____ is the full form of BIOS. *1*

SECTION B

*Answer all **five** very short answer type questions.*

11. What are the techniques for obtaining and exploiting personal information for identity theft ? *2*

12. What is File carving and Bluesnarfing ? *2*

13. What is the difference between "copy of the drive" and "imaging of the drive" ? *2*

14. What is electronic tampering ? *2*

15. Define Windows Registry. Why is it important for forensics ? *2*

SECTION C

*Answer any **two** questions out of three short answer type questions.*

16. How can deleted data be retrieved from a PC ? How is it possible to know what Internet sites have been visited ? *5*

17. Explain any digital forensic investigation model. *5*

18. Describe procedures for acquiring data from cell phones and mobile devices. *5*

SECTION D

*Answer any **two** questions out of three long answer type questions.*

19. How is digital evidence processed ? What are the steps involved in Evidence Acquisition ? Explain with the help of hypothetical case. *10*

20. What is the difference between WiFi and WiMax ? Specify their standards, technical characteristics and security policies. *10*

21. What are the issues involved with detection of cyber-crimes in India ? *10*

No. of Printed Pages : 3

M01864

MSEI-027

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination,

December 2019

MSEI-027 : DIGITAL FORENSICS

Time : 2 Hours] *[Maximum Marks : 50*

Note : (i) Section - A :- Answer all the objective type questions.

(ii) Section - B :- Answer all the very short answer type questions.

*(iii) Section - C :- Answer **any two** questions out of three short answer type questions.*

*(iv) Section - D :- Answer **any two** questions out of three long answer type questions.*

Section - A

Attempt all the questions.

1. Ubuntu is also _____. 1

2. WAP stands for Wired Application protocol 1
   a) True
   b) False

3. EDGE stands for enhanced Data Rate for GSM Environment. 1
   a) True
   b) False

4. HTTP stands for "Hyper Text Technical Protocol" 1
   a) True
   b) False

5. TCP/IP protocol used behind ping command 1
   a) True
   b) False

6. "TFTP" stands for _____. 1

7. DDOS stands for _____. 1

8. "SSIDs" stands for _____. 1

9. PDA stands for _____. 1

10. The name of Website containing periodic posts _____. 1

Section - B

(Five very short answer type questions)

Attempt all questions.

11. What is CDR? How it helps for Investigation? 2

12. Explain the difference between "Line acquisition" and "Post mortem acquisition". 2

13. What is CoC (Chain of Custody)? 2

14. What are the different formats for digital evidence? 2

15. Explain Salvaging of data. 2

Section - C

(Attempt **two** out of **three** short answer type questions)

16. What are the legal issues involved in seizure of the computer equipment? 5

17. What is IMEI? Why it is used in Mobile phone devices? How it is helpful in forensic investigation? 5

18. Explain any two tools used in "Forensic examination of Mobile devices". 5

Section - D

(Attempt **two** out of **three** long answer type questions)

19. What is the general process for conducting a digital investigation? 10

20. What are the counterfeit documents? What are the steps involved in detection of counterfeit document? Give a brief note on the duties performed by the examiner. 10

21. Write short notes on the following: 5×2=10
    a) Harassment
    b) Admissible evidence
    c) SIM card acquisition
    d) Cyber bullying
    e) Human trafficking

✧✧✧✧✧✧

No. of Printed Pages : 5

MSEI-027

P. G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

June, 2020

MSEI-027 : DIGITAL FORENSICS

Time : 2 Hours *Maximum Marks : 50*

Note : ***Section A :*** *Answer all the objective questions.*

Section B : *Answer all the very short answer questions.*

Section C : *Answer any two questions out of three short answer type questions.*

Section D : *Answer any two questions out of three long answer type questions.*

Section—A

(Objective Type Questions)

Note : *Attempt all questions.*

1. The first step in a digital forensic process is 1

2. When performing a forensic analysis, what device is used to prevent the system from recording data on an evidence disk ? 1

   (a) Write-Blocker

   (b) Protocol analyzer

   (c) Firewall

   (d) Disk Editor

3. ..... is a collection of infected computers or bots that been taken by hackers and are used to perform malicious tasks or functions. 1

4. ..... is a digital object that contains reliable information that supports or refutes a hypothesis. 1

5. ..... is a programming instructions that are complied into the executable files that are sold by software development companies. 1

6. GSM stands for 1

7. ..... is the international or uninternational use of a portable USB mass storage device to illicitly download confidential data from a network endpoint. 1

8. Whenever a system is compromised, there is almost always something left behind by the attacker be it code fragments, trojan programmes, running processes, or sniffer log files. These are known as 1

9. ..... is "an information resource whose value lies in unauthorized or illicit use of that resource". 1

10. TFTP stands for 1

Section—B

(Very Short Answer Questions)

Note : *Attempt all questions.*

11. Explain the advantages of wireless devices. 2

12. Explain the purpose of SHA algorithm. 2

13. Explain the purpose of CAPTCHA. 2

14. Which IT Amendment Act, 2008 Section is applicable for Data theft from Removable Drives ? Suggestions to prevent data theft. 2

15. What is 802.11 Standard ? 2

Section—C

(Short Answer Type Questions)

Note : Attempt any two questions.

16. Explain the different parameters of Log File Analysis. 5

17. Explain the wireless point security standards. 5

18. Explain the purpose of CDR Analysis while investigations. 5

Section—D

(Long Answer Type Questions)

***Note :** Attempt any **two** questions.*

19. Explain the modes of operation in wireless communications and different categories of WLAN. 10

20. How to implement the file attributes analysis ? What is the process to reconstruct deleted files ? 10

21. What is the difference between dead acquisition, live acquisition and error handling ? 10

No. of Printed Pages : 4

MSEI-027

P. G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

December, 2020

MSEI-027 : DIGITAL FORENSICS

Time : 2 Hours *Maximum Marks : 50*

***Note* : *Section–A* :** *Answer all the objective type questions.*

***Section–B* :** *Answer all the very short answer type questions.*

Section–C* :** *Answer any* ***two *questions out of* ***three*** *short answer type questions.*

Section–D* :** *Answer any* ***two *out of three long answer type questions.*

Section—A

***Note* :** Attempt all the questions. 1 each

1. MD5 use ..... bits encryption and SHA256 use ..... bits encryption.

2. VOIP stands for .....

3. Which file system is used in Linux ?

4. Write a command to create an image of Pendrive using dd command.

5. SNMP stands for ..... .

6. EDGE stands for ..... .

7. Which IEEE standards are used for Bluetooth technology ?

8. IMSI stands for ..... .

9. Spam is the use of electronic messaging system to send unsolicited bulk messages indiscriminately .

   (a) True

   (b) False

10. When examining hard disk without a write-blocker, you should not start windows because windows will write data to the ..... .

    (a) Recycle Bin

(b) Case Files

(c) BIOS

(d) MS DOS sys

Section—B

Note : Attempt all the ***five*** very short answer type questions.

11. Explain the concept of data integrity. 2

12. Explain the concept of file carving. 2

13. Explain the use of RADIUS. 2

14. Explain Man-in-the-Middle attacks. 2

15. Explain the Cyber Bullying. 2

Section—C

Note : Attempt any ***two*** out of three short answer type questions.

16. Explain the *five* rules of collecting electronic evidence. 5

17. How is Money Laundering different from Banking Crime ? 5

18. Explain any ***two*** types of SPAM. 5

Section—D

Note **:** Attempt any ***two*** out of three long answer type questions.

19. Explain any ***three*** WLAN Security Algorithms in detail. 10

20. Explain MAC Spoofing. Explain the concept of Encryption and Steganography. 10

21. Explain file artifacts, file carving, file recovery, magic code and Hash functions with respect to Cyber Forensics. 10