REG. NUMBER:

**NADAR SARASWATHI COLLEGE OF ENGINEERING AND TECHNOLOGY**

**VADAPUDUPATTI, THENI – 625 531**

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**

**INTERNAL EXAM-I**

| | | | | | |
|---|---|---|---|---|---|
| **Subject** | : | Cyber Forensics | **Date & Session** | : | 24/03/23 / FN |
| **Subject Code** | : | CS8074 | **Duration** | : | 90 Min |
| **Year/Sem./Branch** | : | IV/VIII/CSE | **Max. Marks** | : | 50 |

**COURSE OUTCOME**

| | | | |
|---|---|---|---|
| **CO1** | : | Understand the basics of computer forensics | 25 |
| **CO2** | : | Apply a number of different computer forensic tools to a given scenario | 25 |
| | | **WEIGHTAGE** | 50 |

**Part-A (8x2 =16 Marks)**

| | | | | |
|---|---|---|---|---|
| **1** | Define cyber forensics. | L1 | CO1 | **(2)** |
| **2** | Define 'Hacking'. | L1 | CO1 | **(2)** |
| **3** | Discuss RAID Data acquisition. | L1 | CO1 | **(2)** |
| **4** | What is a forensic duplicate ? | L3 | CO1 | **(2)** |
| **5** | Define file carving. | L4 | CO2 | **(2)** |
| **6** | What is virtual machine? | L1 | CO2 | **(2)** |
| **7** | Distinguish between validation and discrimination. | L3 | CO2 | **(2)** |
| **8** | Define Master Boot Record (MBR) | L1 | CO2 | **(2)** |

**Part-B ( 2 x 12= 24 Marks)**

| | | | | |
|---|---|---|---|---|
| **9. A** | Demonstrate how to use remote network acquisition tools in cyber forensics. | L3 | CO1 | **(12)** |
| | **[OR]** | | | |
| **9. B** | Explain in detail about Incident and Incident Response Methodology | L1 | CO1 | **(12)** |
| **10. A** | Analyze how the following techniques are used :<br>(i) Documents evidence in the lab<br>(ii) Processing and handling Digital evidence | L3 | CO2 | **(12)** |
| | **[OR]** | | | |
| **10. B** | Explain in details the various computer forensic tools. | L2 | CO2 | **(12)** |

**PART C (1x10=10)**

| | | | | |
|---|---|---|---|---|
| **11** | i) Explain the Stages of Investigative Process of Digital Forensics<br>ii)While processing crime, how will you work with windows and DOS systems ? | L1 | CO1 & CO2 | **(5)**<br>**(5)** |


REG. NUMBER:

NADAR SARASWATHI COLLEGE OF ENGINEERING AND TECHNOLOGY

VADAPUDUPATTI, THENI – 625 531

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

INTERNAL EXAM-I

| | | | | | |
|---|---|---|---|---|---|
| **Subject** | : | Cyber Forensics | **Date & Session** | : | 24/03/23 / FN |
| **Subject Code** | : | CS8074 | **Duration** | : | 90 Min |
| **Year/Sem./Branch** | : | IV/VIII/CSE | **Max. Marks** | : | 50 |

**COURSE OUTCOME**

| | | | |
|---|---|---|---|
| **CO1** | : | Understand the basics of computer forensics | 25 |
| **CO2** | : | Apply a number of different computer forensic tools to a given scenario | 25 |
| | | **WEIGHTAGE** | 50 |

**Part-A (8x2 =16 Marks)**

| | | | | |
|---|---|---|---|---|
| **1** | Define cyber forensics. | L1 | CO1 | **(2)** |
| **2** | Define 'Hacking'. | L1 | CO1 | **(2)** |
| **3** | Discuss RAID Data acquisition. | L1 | CO1 | **(2)** |
| **4** | What is a forensic duplicate ? | L3 | CO1 | **(2)** |
| **5** | Define file carving. | L4 | CO2 | **(2)** |
| **6** | What is virtual machine? | L1 | CO2 | **(2)** |
| **7** | Distinguish between validation and discrimination. | L3 | CO2 | **(2)** |
| **8** | Define Master Boot Record (MBR) | L1 | CO2 | **(2)** |

**Part-B ( 2 x 12= 24 Marks)**

| | | | | |
|---|---|---|---|---|
| **9. A** | Demonstrate how to use remote network acquisition tools in cyber forensics. | L3 | CO1 | **(12)** |
| | **[OR]** | | | |
| **9. B** | Explain in detail about Incident and Incident Response Methodology | L1 | CO1 | **(12)** |
| **10. A** | Analyze how the following techniques are used :<br>(i) Documents evidence in the lab<br>(ii) Processing and handling Digital evidence | L3 | CO2 | **(12)** |
| | **[OR]** | | | |
| **10. B** | Explain in details the various computer forensic tools. | L2 | CO2 | **(12)** |

**PART C (1x10=10)**

| | | | | |
|---|---|---|---|---|
| **11** | i) Explain the Stages of Investigative Process of Digital Forensics<br>ii)While processing crime, how will you work with windows and DOS systems ? | L1 | CO1 & CO2 | **(5)**<br>**(5)** |