

SYLLABUS

POST GRADUATE DIPLOMA IN
DIGITAL FORENSICS



ENLIGHTENMENT TO PERFECTION
2024 -- 2025

University of North Bengal

OUTLINE OF COURSE STRUCTURE

Post Graduate Diploma in Digital Forensic

(Session: 2024-25)

SEMESTER-I

| Course Code | Name of the module | Marks | Credit | Hours/Week |
|--|--|------------|-----------|------------|
| Course (Theoretical) | | | | |
| DFPGD-101 | Window Forensics and Linux Forensics | 40 | 2 | 4 |
| DFPGD-102 | Defeating Anti-Forensics Techniques | 40 | 2 | 4 |
| DFPGD-103 | Network Forensics | 40 | 2 | 4 |
| Course (Practical) | | | | |
| DFPGD-104 | Window Forensics and Linux Forensics Lab | 40 | 2 | 5 |
| DFPGD-105 | Mobile Forensics Lab | 40 | 2 | 5 |
| DFPGD-106 | Network Forensics Lab | 40 | 2 | 5 |
| Continuing Evaluation | | | | |
| DFPGD-107 | Exam | 15 | 2 | 2 |
| DFPGD-108 | Project | 45 | 2 | 1 |
| Total Marks & Credits in the Semester I | | 300 | 16 | 30 |

Semester-II

| Course Code | Name of the module | Marks | Credit | Hours/Week |
|---|------------------------|------------|-----------|------------|
| Course (Theoretical) | | | | |
| DFPGD-201 | Dark Web Forensics | 40 | 2 | 4 |
| DFPGD-202 | Hardware Forensics | 40 | 2 | 4 |
| DFPGD-203 | Malware Forensics | 40 | 2 | 4 |
| Course (Practical) | | | | |
| DFPGD-204 | Dark Web Forensics Lab | 40 | 2 | 5 |
| DFPGD-205 | Hardware Forensics Lab | 40 | 2 | 5 |
| DFPGD-206 | Malware Forensics Lab | 40 | 2 | 5 |
| Continuing Evaluation | | | | |
| DFPGD-207 | Exam | 15 | 2 | 1 |
| DFPGD-208 | Project | 15 | 1 | 1 |
| DFPGD-209 | Internship | 30 | 1 | 1 |
| Total Marks & Credits in the semester II | | 300 | 16 | 30 |
| Grand Total | | 600 | 32 | 60 |

Detailed Syllabus

Semester-I

| Course Code | Name of the module | Marks |
|------------------|------------------------------------|-----------|
| DFPGD-101 | WINDOW FORENSIC AND LINUX FORENSIC | 40 |

| UNIT 1 | WINDOW FORENSIC |
|--------|---|
| | <ol style="list-style-type: none">1. Volatile and Non-Volatile Information2. Windows Memory and Registry Analysis3. Cache, Cookie, and History Recorded in Web Browsers4. Windows Files and Metadata |

| UNIT 2 | LINUX FORENSIC |
|--------|---|
| | <ol style="list-style-type: none">1. Volatile and Non-Volatile Data in Linux2. Analyze Filesystem Images Using The Sleuth Kit3. Memory Forensic4. Mac Forensic |

| DFPGD-102 | DEFEATING ANTI-FORENSICS TECHNIQUES | 40 |
|-----------|--|----|
| UNIT 3 | <ol style="list-style-type: none">1. Disk Wiping2. File Encryption3. Steganography4. Compression5. Memory Resident Compiler / Assemblers | |

| DFPGD-103 | NETWORK FORENSIC | 40 |
|-----------|---|----|
| UNIT 4 | <ol style="list-style-type: none">1. Network Forensics Fundamentals2. Event Correlation Concepts And Types3. Identify Indicators of Compromise (Iocs) From Network Logs4. Investigate Network Traffic | |

| DFPGD-104 | WINDOW AND LINUX FORENSIC PRACTICAL | 40 |
|-----------|--|----|
| | <ol style="list-style-type: none">1. Magnet Encrypted Disk Detector2. Magnet RAM Capture3. FAW(Forensic Acquisition Of Websites) | |

| DFPGD-105 | MOBILE FORENSIC PRACTICAL | 40 |
|-----------|---|----|
| | <ol style="list-style-type: none">1. Cellebrite UFED(Universal Forensic Extraction Device)2. Oxygen Forensic Detective3. MSAB XRY | |

DFPGD-106

NETWORK FORENSIC PRACTICAL

40

1. NMAP
2. Network Miner
3. Snort

DFPGD-107

Continuing Evaluation

EXAM

PROJECT

Semester -II

| Course Code | Name of the module | Marks |
|-----------------------------------|--|-----------|
| DFPGD-201 <i>Unit-1</i> | DARK WEB FORENSICS 1. Dark Web 2. Dark Web Forensics 3. Tor Browser Forensics 4. Dark Web Artifacts 5. Dark Web Threats | 40 |
| DFPGD-202 <i>Unit-2</i> | HARDWARE FORENSICS 1. Introduction To Hardware Forensics 2. Computer Hardware Fundamentals 3. Peripheral Devices and Forensic 4. Embedded Systems and IoT Devices | 40 |
| DFPGD-203 <i>Unit-3</i> | MALWARE FORENSICS 1. Introduction To Malware 2. Malware Analysis Fundamentals 3. Malware Detection and Prevention Techniques 4. Static Malware Analysis 5. Dynamic Malware Analysis 6. Memory Forensics For Malware Analysis 7. Malware Forensics For Malware Analysis 8. Malware Reverse Engineering 9. Web Based Malware 10. Incident Response and Handling Malware Incidents | 40 |
| DFPGD-204 | Dark Web Forensics (Practical) ✓ Tor Browser | 40 |
| DFPGD-205 | Hardware Forensics (Practical) ✓ Laptop Device Hardware Forensics ✓ Motherboard and Hard Disk Forensics | 40 |
| DFPGD-206 | Malware Forensics (Practical) ✓ IDA Pro ✓ OllyDbg ✓ Wireshark ✓ Volatility ✓ REMux ✓ YARA ✓ CAPE | 40 |
| DBI-207 | Continuing Evaluation Educational Trip along with submission of a final tour report | 15 |
| DBI-208 | Continuing Evaluation Class Tests | 15 |