QualityThought®
Transforming Dreams! Redefining Future!

CELEBRATING 15 YEARS

Malware Analysis & Digital Forensic

88974 86382, 88858 78710 | #302, Nilgiri Block, Aditya Enclave, Ameerpet, Hyd.,Telangana-500016
qualitythought.in | ihubtalent.com

QualityThought®
Transforming Dreams! Redefining Future!

CELEBRATING 15 YEARS

Introduction to Malware

- Malware types (Trojan, Ransomware, RATs, Worms, etc.)
- Malware lifecycle & case studies

Malware Analysis Environment Setup

- VirtualBox, isolated networks, INetSim, and safety tips
- Tools: ProcMon, TCPView, PEStudio, Wireshark

Static Malware Analysis

- Hashing, strings, metadata, PE file structure
- Using PEStudio, ExeInfoPE

Behavioral Analysis (Dynamic)

- Monitoring file, registry, process changes
- Tools: ProcMon, RegShot, Process Hacker

Network Behavior Analysis

- Packet capture (Wireshark), C2 detection basics
- DNS, HTTP/HTTPS-based malware activity

Advanced Malware Techniques

- Focus: Real-world malware traits, persistence, and sandboxing

Malware Execution Flow

- Process injection, child process creation
- Windows API behaviors (overview only)

Malware Evasion Techniques

- Anti-VM, anti-debugging, obfuscation methods
- Detecting behavior-based evasion

Malware Persistence Techniques

- Registry run keys, scheduled tasks, WMI
- Identifying persistence indicators

Analyzing Droppers & Downloaders

- First-stage vs second-stage malware
- Live sample analysis of dropper behavior

On Malware Case Study

- Analyze one InfoStealer or Trojan
- Deliver IOC report

Incident Response & Malware Reporting

- Focus: End-to-end response process for malware attacks

Malware Log Analysis

- Sysmon, Windows Event logs for malware indicators
- IOC correlation

Malware Triage & Containment

- Initial triage, isolation strategy
- Tools/scripts for quick containment

Malware Investigation Report Writing

- Format: Executive summary, IOCs, behavior, recommendations
- Templates for incident reporting

Group Activity – Malware IR Simulation

- Simulated infection chain
- Analyze and contain threat as a team

Malware Analysis Assessment & Recap

- Quiz + Practical
- Recap key tools, workflow, tips

Digital Forensics

Forensics Fundamentals

- Focus: Core forensic concepts, acquisition, and legal aspects

Introduction to Digital Forensics

- Scope, phases, and challenges
- Volatile vs non-volatile data

Evidence Handling & Chain of Custody

- Legal considerations, tools for documentation
- Disk imaging tools (FTK Imager)

File System Forensics – Windows

- NTFS structure, MFT, $Logfile, $UsnJrnl
- Data carving concepts

Forensic Imaging & Validation

- Creating disk images
- Hashing for integrity check

Lab: Disk Acquisition + File System Analysis

- Use FTK Imager + Autopsy
- Identify deleted files, access patterns

Host, Email, and Browser Forensics

- Focus: System artifact analysis for evidence discovery

Memory Forensics (Volatility Basics)

- Memory acquisition tools
- Volatility: pslist, malfind, cmdscan,

Windows Artefacts – Deep Dive

- Prefetch, Jump Lists, LNK, Shimcache
- Extracting user behavior

Email Forensics

- Header analysis, phishing trace, email payload
- Tools: PST Viewer, online analyzers

Browser & Application Forensics

- Chrome/Firefox history, cache, cookies
- Tools: NirSoft utilities, SQLite viewers

Lab: Email + Browser + Artefact Analysis

- Forensic case scenario
- Student creates mini forensic report

End-to-End Investigation

- Focus: Combining skills for timeline building and reporting

Timeline Analysis

- Creating forensic timeline using Plaso/log2timeline
- Event correlation

Incident Response Process

- Triage → Containment → Analysis → Recovery
- Documentation and SOPs

Capstone Briefing: Forensic Case

- Provide compromised image (Windows or Linux)
- Objectives: find infection vector, timeline, user activity

Student Project + Reporting

- Investigation + Report submission
- Peer reviews and feedback

Final Day: Career Tips + Certification Paths

- CHFI, GCFA, EnCE overview
- Resume building & job roles in DFIR

Tools Covered

Malware Analysis Tools

- PEStudio, ExeInfoPE, ProcMon, RegShot, Wireshark, Process Hacker

Forensics Tools

- FTK Imager, Autopsy, Volatility, Plaso, Browser History Viewer, PST Viewer

Our Students Are Placed In

TCS · Capgemini · LTIMindtree · accenture
CLOUD9 · CloudCover · Coforge · CGI · CISCO · Cloud4C · amazon
databricks · dataflex · DXC TECHNOLOGY · Cognizant · Convergytics · CSS CORP · Medtronic
genpact · HCL · HSBC · Deloitte. · EMIDS · Foray · STIC Soft
Infosys · Legato · MINDGRAPH · Mindtree · motivitylabs · photon · meslova
pwc · quantiphi · RENAULT · SIGMASOFT · SOFTILITY · syren cloud · splashBI
TIGER ANALYTICS · wipro · ENVISION · virtusa · ValueLabs · zensor. · SOLIX
JRD SYSTEMS · ValueLabs · archents · magnasoft · Innominds · techforce.ai · techolution

QualityThought

88974 86382, 88858 78710

Quality Thought Infosystems India (P) Ltd.

#302, Nilgiri Block, Ameerpet, Hyderabad-500016 | www.qualitythought.in | info@qualitythought.in