

# A Detailed Analysis of an Advanced Persistent Threat Malware

By Created by:Frankie Fu Kay Li

Archived: 2026-04-05 19:25:58 UTC

[Download File](#)

A Detailed Analysis of an Advanced Persistent Threat Malware (PDF, 4.44MB)Published: 14 Oct, 2011

Spear-phishing emails were sent to a political figure at my place of residence. An email together with the attached sample was provided for forensics analysis. It appears to be an Advanced Persistent Threat type malware. By performing behavioral and code analysis in an alternatively way, most of its important functions were identified. The aim of this technical paper is to illustrate the detailed procedures of how this malware was dissected.

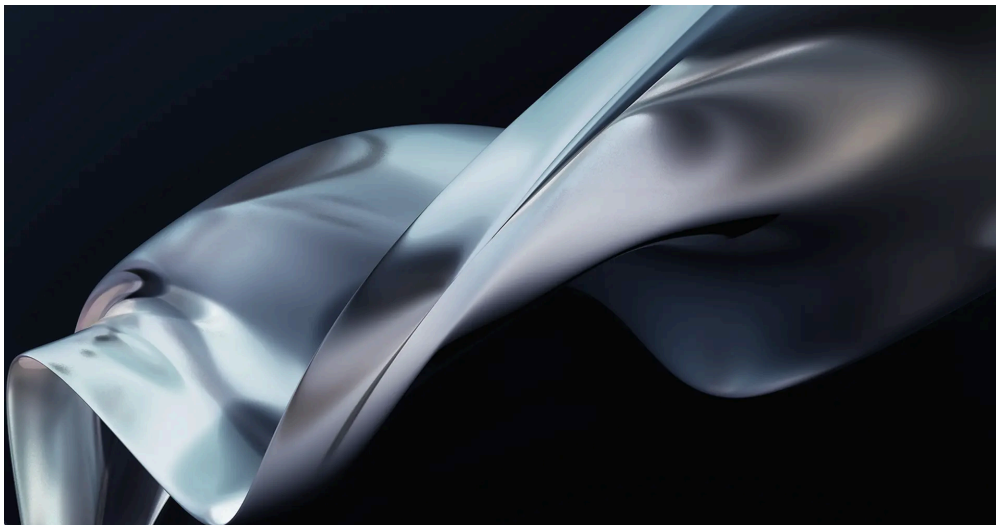
## Additional resources

## Related courses

- Slide 1 of 16

### **FOR589: Cybercrime Investigations**

FOR589Digital Forensics and Incident Response



- 5 Days (Instructor-Led)
- 30 CPEs / 30 Hours (Self-Paced)

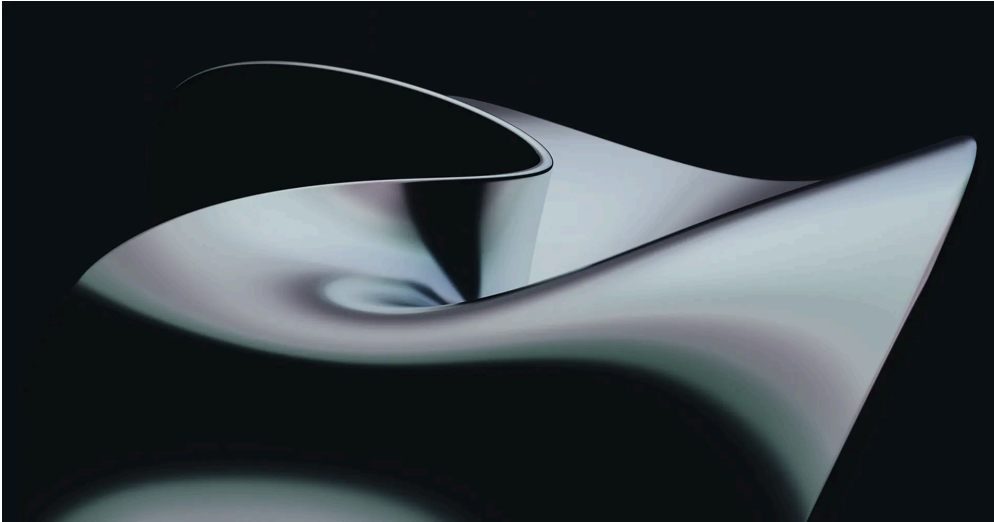
- Labs: 20 Hands-On Labs

[View course details](#)[Register](#)

- Slide 2 of 16

### **FOR585: Smartphone Forensic Analysis In-Depth**

FOR585 Digital Forensics and Incident Response



- GIAC Advanced Smartphone Forensics (GASF)
- 6 Days (Instructor-Led)
- 36 CPEs / 36 Hours (Self-Paced)
- Labs: 22 Hands-On Labs

[View course details](#)[Register](#)

- Slide 3 of 16

### **FOR478: Cyber Threat Intelligence Foundations**

FOR478 Digital Forensics and Incident Response



- 2 Days (Instructor-Led)
- 16 CPEs / 16 Hours
- Labs: 8 Hands-On Labs

[View course details](#)[Register](#)

- Slide 4 of 16

## **FOR608: Enterprise-Class Incident Response & Threat Hunting**

FOR608 Digital Forensics and Incident Response



- GIAC Enterprise Incident Responder (GEIR)
- 6 Days (Instructor-Led)
- 36 CPEs / 36 Hours (Self-Paced)
- Labs: 20 Hands-On Labs

[View course details](#)[Register](#)

- Slide 5 of 16

### **FOR518: Mac and iOS Forensic Analysis and Incident Response**

FOR518Digital Forensics and Incident Response



- GIAC iOS and macOS Examiner (GIME)
- 6 Days (Instructor-Led)
- 36 CPEs / 36 Hours (Self-Paced)
- Labs: 23 Hands-On Labs

[View course details](#)[Register](#)

- Slide 6 of 16

### **FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics**

FOR508Digital Forensics and Incident Response



- GIAC Certified Forensic Analyst (GCFA)
- 6 Days (Instructor-Led)
- 36 CPEs / 36 Hours (Self-Paced)
- Labs: 35 Hands-On Labs

[View course details](#)[Register](#)

- Slide 7 of 16

## **FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques**

FOR610 Digital Forensics and Incident Response



- GIAC Reverse Engineering Malware (GREM)
- 6 Days (Instructor-Led)
- 36 CPEs / 36 Hours (Self-Paced)
- Labs: 48 Hands-On Labs

[View course details](#)[Register](#)

- Slide 8 of 16

### **FOR578: Cyber Threat Intelligence**

FOR578 Digital Forensics and Incident Response



- GIAC Cyber Threat Intelligence (GCTI)
- 6 Days (Instructor-Led)
- 36 CPEs / 36 Hours (Self-Paced)
- Labs: 20 Hands-On Labs

[View course details](#)[Register](#)

- Slide 9 of 16

### **FOR509: Enterprise Cloud Forensics and Incident Response**

## FOR509 Digital Forensics and Incident Response



- GIAC Cloud Forensics Responder (GCFR)
- 6 Days (Instructor-Led)
- 36 CPEs / 36 Hours (Self-Paced)
- Labs: 23 Hands-On Labs

[View course details](#)[Register](#)

- Slide 10 of 16

## FOR528: Ransomware and Cyber Extortion

### FOR528 Digital Forensics and Incident Response



- 4 Days (Instructor-Led)
- 24 CPEs / 24 Hours (Self-Paced)
- Labs: 13 Hands-On Labs

[View course details](#)[Register](#)

- Slide 11 of 16

### **FOR577: LINUX Incident Response and Threat Hunting**

FOR577Digital Forensics and Incident Response



- GIAC Linux Incident Responder (GLIR)
- 6 Days (Instructor-Led)
- 36 CPEs / 36 Hours (Self-Paced)
- Labs: 23 Hands-On Labs

[View course details](#)[Register](#)

- Slide 12 of 16

### **FOR710: Reverse-Engineering Malware: Advanced Code Analysis**

FOR710Digital Forensics and Incident Response



- 36 CPEs / 36 Hours (Self-Paced)
- Labs: 12 Hands-On Labs

[View course details](#)[Register](#)

- Slide 13 of 16

### **FOR498: Digital Acquisition and Rapid Triage**

FOR498 Digital Forensics and Incident Response



- GIAC Battlefield Forensics and Acquisition (GBFA)

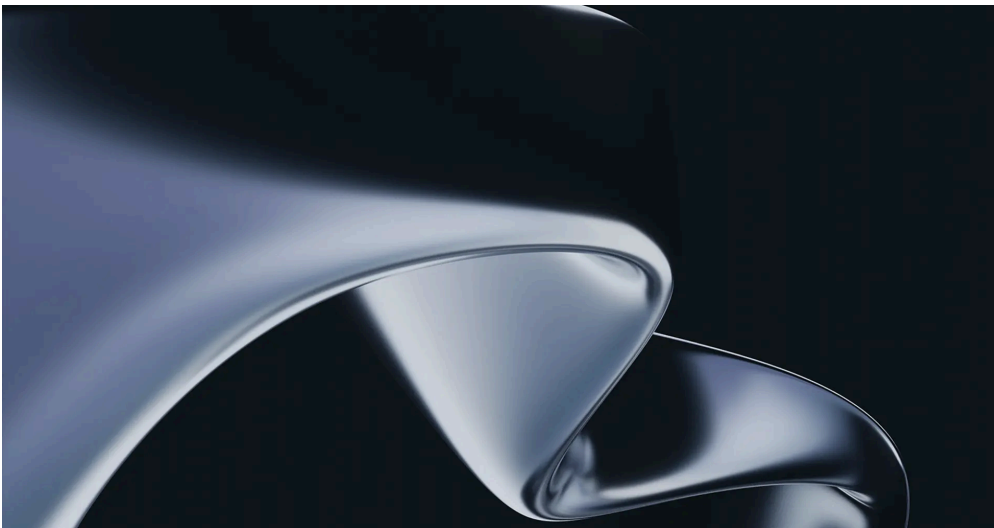
- 6 Days (Instructor-Led)
- 36 CPEs / 36 Hours (Self-Paced)
- Labs: 20 Hands-On Labs

[View course details](#)[Register](#)

- Slide 14 of 16

### **FOR563: Applied AI for Digital Forensics and Incident Response: Leveraging Local Large Language Models**

FOR563 Digital Forensics and Incident Response, Artificial Intelligence



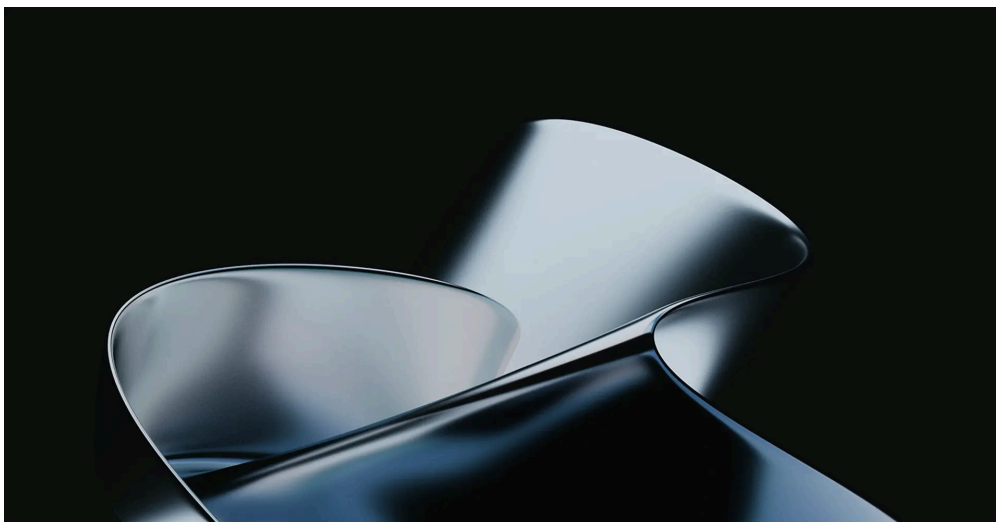
- 1 Day (Instructor-Led)
- 6 CPEs / 6 Hours (Self-Paced)
- Labs: 4 Hands-On Labs

[View course details](#)[Register](#)

- Slide 15 of 16

### **FOR500: Windows Forensic Analysis**

FOR500 Digital Forensics and Incident Response



- GIAC Certified Forensic Examiner (GCFE)
- 6 Days (Instructor-Led)
- 36 CPEs / 36 Hours (Self-Paced)
- Labs: 22 Hands-On Labs

[View course details](#)[Register](#)

- Slide 16 of 16

## **FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response**

FOR572 Digital Forensics and Incident Response



- GIAC Network Forensic Analyst (GNFA)
- 6 Days (Instructor-Led)
- 36 CPEs / 36 Hours (Self-Paced)
- Labs: 20 Hands-On Labs

[View course details](#)[Register](#)

---

Source: <https://www.sans.org/white-papers/33814/>