Cybercrime Investigations: Digital Forensics for Cybersecurity Professionals

Helping Cybercrime Lawyers Through Technical Expertise

Introduction – What is Digital Forensics ?

Digital Forensics is the process of:

- ✓ Identifying
- ✓ Preserving
- ✓ Analyzing, and
- ✓ Presenting

Digital evidence in investigations involving cybercrime, fraud, data breaches, or unauthorized access. It helps law enforcement agencies, businesses, and security professionals uncover malicious activities, track cybercriminals, and protect sensitive data.

Key Aspects of Digital Forensics

- ✓ **Computer Forensics** – Examining devices like computers, hard drives, and storage media for evidence.
- ✓ **Network Forensics** – Investigating network traffic to detect security breaches and cyberattacks.
- ✓ **Memory Forensics** – Analyzing system memory to uncover live-running processes and threats.
- ✓ **Malware Analysis** – Understanding malicious software behavior to develop security countermeasures.
- ✓ **Forensic Tools & Techniques** – Using specialized software such as EnCase, FTK, and Sleuth Kit for evidence collection and analysis.

Why Digital Forensics Matters

1. Cybercrime Investigation
2. Evidence Authenticity & Integrity
3. Security Enhancement
4. Hidden Data Discovery
5. Financial & Reputational Protection

আধুনিক সাইবার নিরাপত্তা এবং আইন প্রয়োগে Digital Forensics কেন গুরুত্বপূর্ণ? ?

Digital Forensics গুরুত্বপূর্ণ কারণ এটি সাইবার অপরাধ, প্রতারণা এবং অননুমোদিত অ্যাক্সেস চিহ্নিত করতে সহায়তা করে। এটি ডিজিটাল প্রমাণ সংরক্ষণ ও বিশ্লেষণের মাধ্যমে আইন প্রয়োগে সহায়ক ভূমিকা রাখে, সাইবার নিরাপত্তা শক্তিশালী করে এবং সংবেদনশীল ডেটা রক্ষা করে।

Key Challenges In Cybercrime Investigations

1. Anonymity & Attribution Issues
2. Jurisdiction & Legal Complexities
3. Volatility of Digital Evidence
4. Advanced Encryption & Hidden Data
5. AI-Powered Cybercrime Evolution
6. Emerging Threats in Cryptocurrency Fraud
7. **Shortage of Cybersecurity Experts**
8. **Resource Constraints & Costly Tools**

Affordable Solutions For 7 & 8 Points

- ➔ Skill Development for Beginners and Experts
- ➔ Affordable Training
- ➔ Hands-On Experience
- ➔ Community Collaboration
- ➔ Continuous Learning

https://tryhackme.com

https://www.hackthebox.com

The Biggest Reasons to Use The Web Platforms Mentioned In Previous Slide?

1. Accessibility of current study materials
2. Expensive CyberSec in a affordable package
3. Networking and experience certified profile

Case Study – Bangladesh Bank Heist – A Cybercrime Landmark

$1 billion

Amount attempted to be stolen through fraudulent transactions, stole $81 Million

Nation-State Attack: Highly sophisticated cyber heist linked to Lazarus Group

SWIFT System Exploitation: Hackers manipulated global banking network

Legal & Jurisdiction Challenges: Cross-border complexities in investigation

Case Study – Bangladesh Bank Heist – How the Hackers Gained Access ?

1. Compromised Network: Attackers infiltrated Bangladesh Bank's internal systems months before the actual heist
2. Malware Deployment: Sophisticated malware planted to manipulate SWIFT transactions
3. Credential Theft: Hackers stole login credentials of banking officials
4. Delayed Detection: Attack went unnoticed due to silent monitoring for weeks

Case Study – Bangladesh Bank Heist – Exploiting the SWIFT System

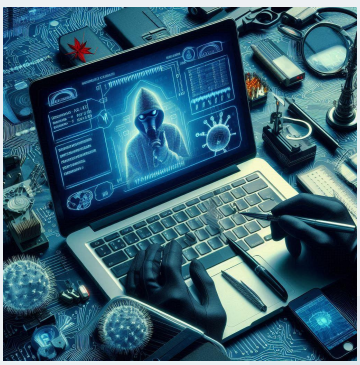
1. Unauthorized SWIFT Transactions: Hackers issued fake payment orders
2. Funds Routed Globally: Money sent to multiple bank accounts in Philippines & Sri Lanka
3. Disguised Transfers: Transactions disguised as legitimate remittances
4. Timing Manipulation: Attack carried out on a Friday to delay response due to weekend closures

Case Study – Bangladesh Bank Heist – Erasing Digital Evidence

1. Log Tampering: Attackers deleted transaction logs to cover their tracks
2. Advanced Encryption: Used to evade forensic detection
3. Fake Printer Malfunction: Hackers disabled transaction printers to prevent alerts
4. Delayed Response: By the time red flags were raised, funds were laundered

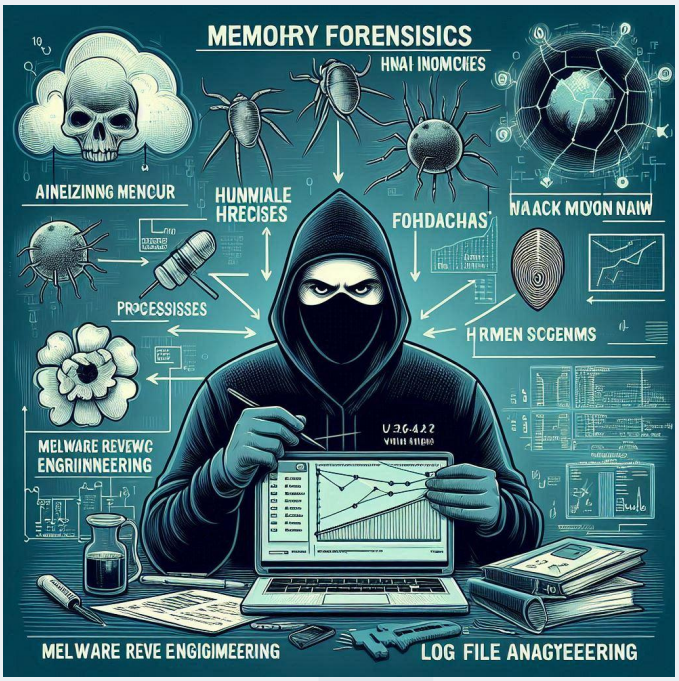
Case Study – Bangladesh Bank Heist –
Lessons Learned

1. AI-Powered Threat Detection: Automating early detection to prevent cybercrime
2. Strengthening SWIFT Security: Multi-factor authentication & continuous monitoring
3. Forensic Intelligence & Log Preservation: Enhancing evidence tracking & secure communication
4. Global Cybercrime Cooperation: Faster international response & unified legal frameworks
5. Continuous Learning & Ethical Hacking Training



Essential Digital Forensic Techniques

- **Memory Forensics**: Analyzing volatile memory to uncover running processes and data.
- **Network Forensics**: Investigating network traffic to identify malicious activities and breaches.
- **Malware Reverse Engineering**: Dissecting malware to understand its behavior and origin.
- **Log File Analysis**: Examining logs to trace user activities and detect anomalies.
- **Forensic Tools**: Tools such as **EnCase**, **FTK**, and **Sleuth Kit** are essential for conducting thorough investigations.



Are there any specific topics you'd like to dive deeper into, such as memory forensics or malware reverse engineering?

Memory Forensics – Steps to Investigate

- **Capture Memory Dump:** Use tools like Volatility & Rekall
- **Analyze Running Processes:** Identify suspicious applications and malware
- **Extract Network Connections:** Detect unauthorized remote access
- **Recover Hidden Artifacts:** Search for encryption keys, hidden files, and credentials

https://volatilityfoundation.org

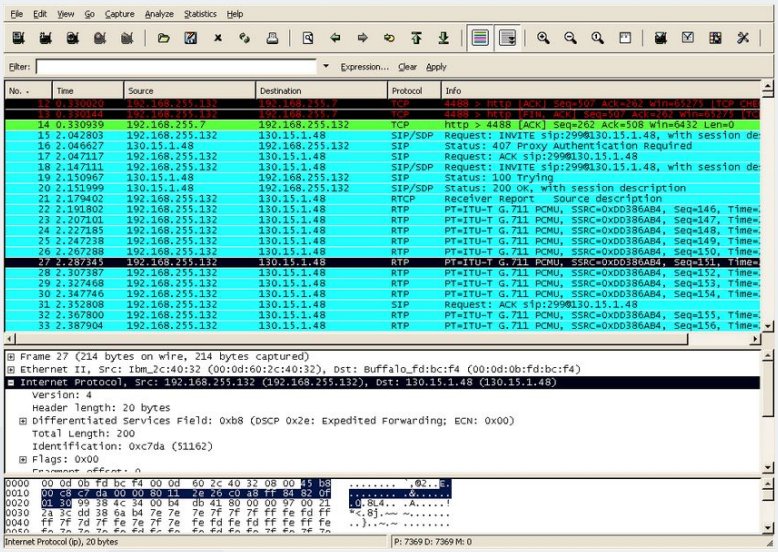
Memory Forensics – Sample Data

```
Terminal
..... 0xffff8c88b39f1580:ApplicationFra          5064    868      3      0 2018-08-30 13:59:43 UTC+0000
..... 0xffff8c88b16b8580:backgroundTask          6664    868      0 ------ 2018-08-30 13:53:51 UTC+0000
..... 0xffff8c88aee73580:backgroundTask          7444    868      0 ------ 2018-08-30 13:54:00 UTC+0000
..... 0xffff8c88af498080:iexplore.exe            9152    868     10      0 2018-08-30 13:54:58 UTC+0000
...... 0xffff8c88af542080:iexplore.exe           8508   9152     17      0 2018-08-30 13:54:59 UTC+0000
..... 0xffff8c88b173a080:backgroundTask          6800    868      0 ------ 2018-08-30 13:53:54 UTC+0000
..... 0xffff8c88aeec6080:ShellExperienc           660    868     19      0 2018-08-30 13:53:46 UTC+0000
..... 0xffff8c88b3999080:SettingSyncHos          4976    868      3      0 2018-08-31 07:52:27 UTC+0000
..... 0xffff8c88af5bb080:RuntimeBroker.          6988    868      3      0 2018-08-30 14:00:00 UTC+0000
..... 0xffff8c88afb2c080:RuntimeBroker.          4860    868      2      0 2018-08-30 13:59:44 UTC+0000
..... 0xffff8c88b585a580:WmiPrvSE.exe            8840    868      4      0 2018-08-30 18:31:10 UTC+0000
..... 0xffff8c88aee88080:backgroundTask          4384    868      0 ------ 2018-08-30 13:54:07 UTC+0000
..... 0xffff8c88b14e7580:WmiPrvSE.exe            2876    868     10      0 2018-08-30 13:52:26 UTC+0000
...... 0xffff8c88b47b9080:powershell.exe         8712   2876     11      0 2018-08-30 16:43:36 UTC+0000
....... 0xffff8c88b12e2080:conhost.exe           1740   8712      4      0 2018-08-30 16:43:36 UTC+0000
....... 0xffff8c88afe2c4c0:powershell.exe        5848   8712      9      0 2018-08-30 16:43:42 UTC+0000
........ 0xffff8c88b2e3a580:rundll32.exe         2216   5848      0 ------ 2018-08-30 22:31:57 UTC+0000
........ 0xffff8c88b1991580:rundll32.exe         8148   5848      0 ------ 2018-08-31 00:56:14 UTC+0000
........ 0xffff8c88b2def580:rundll32.exe         5452   5848      0 ------ 2018-08-30 21:40:18 UTC+0000
........ 0xffff8c88afe0e080:conhost.exe          6572   5848      1      0 2018-08-30 16:43:42 UTC+0000
........ 0xffff8c88afc7c580:cmd.exe              5948   5848      1      0 2018-08-30 22:15:18 UTC+0000
......... 0xffff8c88af412580:conhost.exe         3436   5948      3      0 2018-08-30 22:15:18 UTC+0000
......... 0xffff8c88af601580:p.exe               8260   5948      2      0 2018-08-30 22:15:18 UTC+0000
.......... 0xffff8c88b7...00:rundll32.exe       5768   8260      0 ------ 2018-09-05 12:01:32 UTC+0000
.......... 0xffff8c88b7...80:rundll32.exe       1424   8260      0 ------ 2018-09-06 14:58:41 UTC+0000
.......... 0xffff8c88b7...80:rundll32.exe       7552   8260      0 ------ 2018-09-06 17:26:32 UTC+0000
........ 0xffff8c88b2c42580:rundll32.exe         5588   5848      0 ------ 2018-08-30 21:40:42 UTC+0000
........ 0xffff8c88b2c19080:rundll32.exe         4108   5848      0 ------ 2018-08-30 22:45:25 UTC+0000
........ 0xffff8c88afb184c0:rundll32.exe         6768   5848      0 ------ 2018-08-30 18:31:04 UTC+0000
..... 0xffff8c88b5d4d580:WmiPrvSE.exe            4936    868     12      0 2018-08-30 18:31:17 UTC+0000
..... 0xffff8c88b1374080:SearchUI.exe            5808    868     34      0 2018-08-30 13:53:47 UTC+0000
..... 0xffff8c88af5dc580:RuntimeBroker.          5492    868      2      0 2018-08-30 13:55:14 UTC+0000
..... 0xffff8c88b1aec080:SkypeHost.exe           3964    868     11      0 2018-08-30 13:53:57 UTC+0000
..... 0xffff8c88b3700080:HxTsr.exe               7080    868      0 ------ 2018-08-30 13:53:57 UTC+0000
..... 0xffff8c88afc58080:SystemSettings          5556    868     26      0 2018-08-30 13:59:59 UTC+0000
..... 0xffff8c88b105e4c0:WinStore.App.e          9036    868     33      0 2018-08-30 13:59:43 UTC+0000
..... 0xffff8c88b16cc080:RuntimeBroker.          7136    868      6      0 2018-08-30 13:53:53 UTC+0000
..... 0xffff8c88af65c580:backgroundTask          7656    868      0 ------ 2018-08-30 13:54:01 UTC+0000
.... 0xffff8c88b2fdb580:svchost.exe               988    740     11      0 2018-08-30 13:52:21 UTC+0000
... 0xffff8c88b2bb5580:lsass.exe                  772    632      9      0 2018-08-30 13:52:21 UTC+0000
... 0xffff8c88b2bc5580:fontdrvhost.ex             900    632      5      0 2018-08-30 13:52:21 UTC+0000
. 0xffff8c88b2b43080:smss.exe                     624    388      0 ------ 2018-08-30 13:52:20 UTC+0000
.. 0xffff8c88b2b42080:csrss.exe                   648    624     10      0 2018-08-30 13:52:20 UTC+0000
```

Network Forensics – Steps to Investigate

- **Capture Network Traffic:** Use Wireshark or TCPDump
- **Analyze Suspicious IPs & Protocols:** Detect phishing attempts, DDoS attacks
- **Inspect Encrypted Communication:** Identify SSL/TLS abuse
- **Cross-Check Firewall & IDS Logs:** Detect unauthorized access

Network Forensics – Sample Data



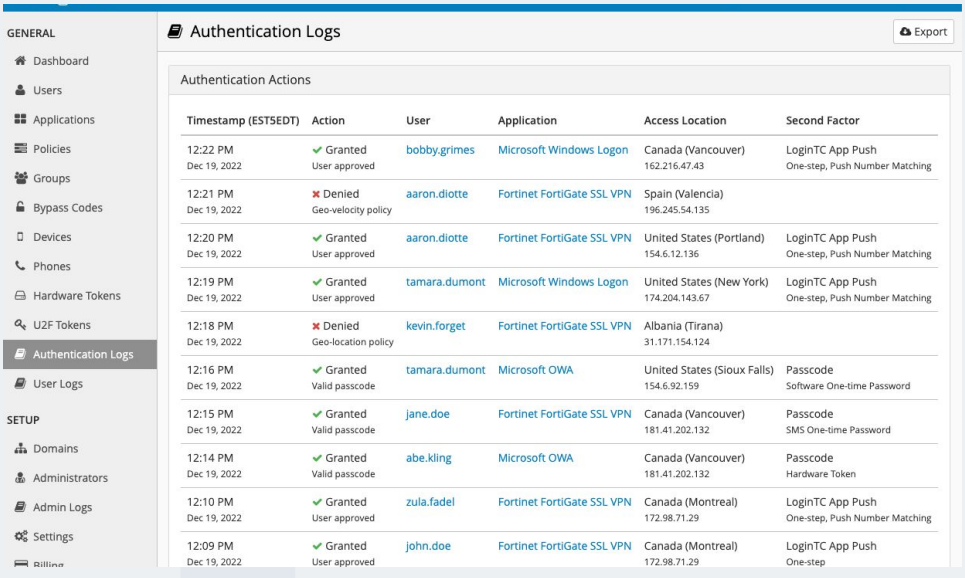
Malware Reverse Engineering – Steps to Investigate

- **Static Analysis:** Examine malware binaries without execution
- **Dynamic Analysis:** Run malware in a sandbox environment
- **Disassemble & Debug:** Analyze source code & executable behavior
- **Trace Persistence Mechanisms:** Identify registry modifications & startup injections

Log File Analysis – Steps to Investigate

- **Extract Authentication Logs:** Identify unauthorized login attempts
- **Analyze System Logs:** Detect anomalies & misconfigurations
- **Correlate Network & Server Logs:** Trace suspicious activities across endpoints
- **Detect Log Tampering:** Identify deleted or altered entries

Log File Analysis – Sample Data



GENERAL
- Dashboard
- Users
- Applications
- Policies
- Groups
- Bypass Codes
- Devices
- Phones
- Hardware Tokens
- U2F Tokens
- Authentication Logs
- User Logs

SETUP
- Domains
- Administrators
- Admin Logs
- Settings
- Billing

Authentication Logs — Export

Authentication Actions

Timestamp (EST5EDT)	Action	User	Application	Access Location	Second Factor
12:22 PM Dec 19, 2022	✓ Granted User approved	bobby.grimes	Microsoft Windows Logon	Canada (Vancouver) 162.216.47.43	LoginTC App Push One-step, Push Number Matching
12:21 PM Dec 19, 2022	✗ Denied Geo-velocity policy	aaron.diotte	Fortinet FortiGate SSL VPN	Spain (Valencia) 196.245.54.135	
12:20 PM Dec 19, 2022	✓ Granted User approved	aaron.diotte	Fortinet FortiGate SSL VPN	United States (Portland) 154.6.12.136	LoginTC App Push One-step, Push Number Matching
12:19 PM Dec 19, 2022	✓ Granted User approved	tamara.dumont	Microsoft Windows Logon	United States (New York) 174.204.143.67	LoginTC App Push One-step, Push Number Matching
12:18 PM Dec 19, 2022	✗ Denied Geo-location policy	kevin.forget	Fortinet FortiGate SSL VPN	Albania (Tirana) 31.171.154.124	
12:16 PM Dec 19, 2022	✓ Granted Valid passcode	tamara.dumont	Microsoft OWA	United States (Sioux Falls) 154.6.92.159	Passcode Software One-time Password
12:15 PM Dec 19, 2022	✓ Granted Valid passcode	jane.doe	Fortinet FortiGate SSL VPN	Canada (Vancouver) 181.41.202.132	Passcode SMS One-time Password
12:14 PM Dec 19, 2022	✓ Granted Valid passcode	abe.kling	Microsoft OWA	Canada (Vancouver) 181.41.202.132	Passcode Hardware Token
12:10 PM Dec 19, 2022	✓ Granted User approved	zula.fadel	Fortinet FortiGate SSL VPN	Canada (Montreal) 172.98.71.29	LoginTC App Push One-step, Push Number Matching
12:09 PM Dec 19, 2022	✓ Granted User approved	john.doe	Fortinet FortiGate SSL VPN	Canada (Montreal) 172.98.71.29	LoginTC App Push One-step

Forensic Tools – Summary of Steps to Investigate

1. **Disk Imaging with EnCase & FTK** → Capture forensic copies of digital evidence

2. **Memory Analysis with Volatility** → Extract live system memory data

3. **Network Forensics with Wireshark** → Analyze packets & network traffic

4. **Log Analysis with SIEM Tools** → Detect anomalies in security logs

How Cybersecurity Professionals Assist Cybercrime Lawyers

Cybersecurity professionals play a vital role in legal cases by:

- Providing expert testimony on digital evidence.
- Assisting with the authentication of digital evidence.
- Ensuring the chain of custody for forensic evidence to maintain its integrity.

Preparing for Cybersecurity Career Paths in Digital Forensics

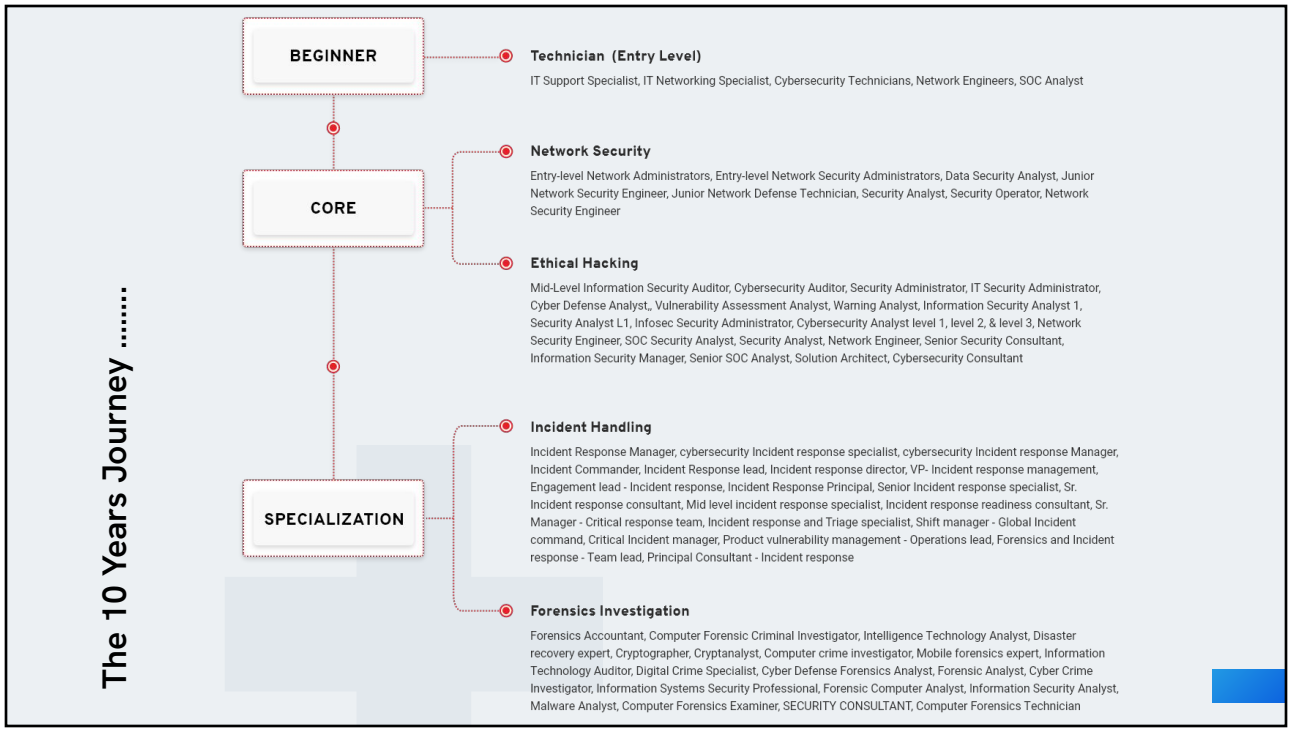
There are various career paths in digital forensics, including:

- **Cyber Forensic Analyst**: Investigates cyber incidents and analyzes evidence.
- **Incident Responder**: Responds to security breaches and mitigates threats.
- **Threat Intelligence Analyst**: Gathers and analyzes information on potential threats.

Preparation Tips:

Search for: **Digital Forensic Learning / Certification Path**
Pursue relevant certifications (e.g., CEH, CCFP).
Gain hands-on experience through internships and labs.
Stay updated on the latest trends and technologies in cybersecurity.

Who is willing to take that career journey ?



Thank you for your time...

A Naser Ahmad
AI in Cybersecurity Researcher

https://www.linkedin.com/in/anaserahmad