Digital Forensics Incident Response Report

Case Number: HTB-SHERLOCK-WFH-001
Report Date: December 12, 2025
Investigator: Nikhil Birla
Lab: HackTheBox Sherlock - "WorkFromHome" DFIR Lab
Lab ID: Sherlock Challenge
Difficulty: Medium
Category: Digital Forensics & Incident Response
Organization: Craw Security

EXECUTIVE SUMMARY

This report details the forensic investigation of the HackTheBox Sherlock "WorkFromHome" laboratory, analyzing a compromised remote employee workstation. The investigation successfully reconstructed a multi-stage attack involving phishing, credential theft, privilege escalation, and persistent malware deployment using EZ Tools (MFTECmd, Registry Explorer), DB Browser for SQLite, and Autopsy.

Laboratory Completion: 24/25 Questions Answered
Unresolved: SHA1 hash of PrintConfig.dll (file securely wiped)
Tools Used: EZ Tools Suite, DB Browser for SQLite, Autopsy 4.19+

INVESTIGATION METHODOLOGY

1. EZ Tools Suite Analysis

MFTECmd Analysis:

- **Command:** MFTECmd.exe -f "$MFT" --csv .
- **Findings:**
    - File deletion timeline for PrintConfig.dll (2025-05-28 12:47:06)
    - Malicious file creation in spool drivers directory
    - Anti-forensic file wiping evidence
    - USN Journal entries showing file system changes

Registry Explorer Analysis:

- **Artifacts Analyzed:** NTUSER.DAT, SYSTEM, SOFTWARE hives
- **Key Findings:**
    - CLSID hijacking: {854A20FB-2D44-457D-992F-EF13785D2B51} → PrintNotify service
    - Wallpaper path: C:/Users/Public/Pictures/gg.bmp in Control Panel\Desktop
    - Persistence mechanisms in Run keys and services
    - Security privilege modifications

2. SQLite Database Analysis (DB Browser)

- **Artifact:** Chrome History database
- **Queries Executed:**

SELECT url, danger_type, interrupt_reason FROM downloads

WHERE url LIKE '%PrintConfig.dll%';

- **Findings:**
    - Download URL: http://freehackingtool.com/tools/PrintConfig.dll
    - danger_type: 7 (DANGEROUS_HOST)
    - interrupt_reason: 41 (THE USER SHUT DOWN BROWSER)
    - state: 2 (INTERRUPTED)

3. Autopsy Analysis

- **Technique:** File carving via MIME type filtering
- **Recovery:** Deleted gg.bmp file containing "HACKED BY ANARCHY"
- **Method:** Images → BMP files → Deleted files recovery

ATTACK TIMELINE (RECONSTRUCTED)

Day 1: Initial Compromise (May 27, 2025)

11:59:57 UTC - RDP session established using stolen credentials

Evidence: Windows Security logs, MFT user profile access

Day 2: Attack Execution (May 28, 2025)

12:00:41 IST - Browser download of PrintConfig.dll blocked by Chrome Safe Browsing

Evidence: Chrome History database, interrupt_reason=41

12:45:37 IST - Successful download via certutil.exe

Evidence: MFT file creation timestamp, certutil execution artifacts

12:47:06 IST - Legitimate PrintConfig.dll deleted

Evidence: MFTECmd deletion timestamp, USN Journal entry

12:54:23 IST - Secondary payload tzres.dll deployed to WBEM directory

Evidence: File creation in C:\windows\system32\wbem\

12:56:11 IST - VBScript hidden attribute set

Evidence: MFT attribute modification timestamp

12:59:30 IST - Desktop wallpaper changed to "HACKED BY ANARCHY"

Evidence: Registry modification, recovered gg.bmp file

15:19:35 IST - Windows Defender detection and quarantine

Evidence: Windows Defender operational logs

CRITICAL EVIDENCE

1. Persistence Mechanism Identified:

- **Service:** PrintNotify
- **CLSID:** {854A20FB-2D44-457D-992F-EF13785D2B51}
- **Method:** DLL search order hijacking
- **Path:** C:\Windows\System32\spool\drivers\x64\3\PrintConfig.dll

2. Browser Forensics Evidence:

- **Phishing URL:** http://login.wowzalnc.co.th/logon.php
- **Block Classification:** DANGEROUS_HOST (type 7)
- **Interrupt Action:** User shut down browser (reason 41)
- **Alternative Delivery:** Certutil.exe as LOLBIN

3. File System Evidence:

- **Malicious Files:** PrintConfig.dll, tzres.dll, a.vbs, gg.bmp
- **Locations:** Spool drivers, WBEM directory, Startup folder, Public Pictures
- **Anti-Forensics:** File deletion, hidden attributes, timestamp manipulation

4. Impact Assessment:

- **Data Accessed:** C:\Users\otello.j\Desktop\Working\Proposal to CFO.pptx
- **System Modified:** Print spooler service, desktop configuration
- **Defacement:** "HACKED BY ANARCHY" wallpaper
- **Privileges Obtained:** SYSTEM via SeManageVolumePrivilege exploit

FORENSIC TECHNIQUES DEMONSTRATED

EZ Tools Proficiency:

- MFT timeline analysis with MFTECmd
- Registry hive parsing with Registry Explorer
- Evidence correlation across multiple artifacts

SQLite Forensics:

- Chrome History database querying
- Download record analysis
- Safe Browsing classification interpretation

File Recovery:

- Deleted file carving with Autopsy
- MIME type-based recovery
- Anti-forensic technique identification

CONCLUSION

The HackTheBox Sherlock "WorkFromHome" laboratory provided comprehensive DFIR training, simulating real-world attack scenarios with anti-forensic challenges. The investigation successfully reconstructed a sophisticated attack chain using professional forensic tools and methodologies. The single unanswered question (SHA1 hash) reflects realistic investigative constraints where evidence may be permanently destroyed.

Skills Validated: Browser forensics, registry analysis, MFT timeline reconstruction, file carving, evidence correlation, professional reporting.

APPENDICES

Appendix A: Forensic Tool Commands & Outputs

1. MFTECmd Analysis Commands

```
# Extract MFT timeline
MFTECmd.exe -f "C\$MFT" --csv . --body full


# Filter for malicious file activity
MFTECmd.exe -f "C\$MFT" --csv . --body full | findstr /i "PrintConfig\|tzres\|gg.bmp"


# USN Journal analysis
MFTECmd.exe -f "C\$Extend\$UsnJrnl" --csv .
```

Key Outputs:

- PrintConfig.dll deleted: 2025-05-28 12:47:06
- tzres.dll created: 2025-05-28 12:54:23
- gg.bmp created: 2025-05-28 12:59:15

2. Registry Explorer Queries

Hives Analyzed:

- C:\Windows\System32\config\SYSTEM
- C:\Windows\System32\config\SOFTWARE
- C:\Users\otello.j\NTUSER.DAT

Key Registry Paths Examined:

HKLM\SYSTEM\CurrentControlSet\Services\PrintNotify

HKLM\SOFTWARE\Classes\CLSID\{854A20FB-2D44-457D-992F-EF13785D2B51}

HKCU\Control Panel\Desktop

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

3. SQLite Database Queries

```
-- Chrome downloads analysis
SELECT datetime(start_time/1000000-11644473600, 'unixepoch') as time,
    url, danger_type, interrupt_reason, state
FROM downloads
WHERE url LIKE '%PrintConfig%' OR url LIKE '%freehackingtool%';

-- Browser history for phishing URL
SELECT datetime(last_visit_time/1000000-11644473600, 'unixepoch') as time,
    url, title, visit_count
FROM urls
WHERE url LIKE '%wowzalnc%' OR url LIKE '%wowzainc%';
```

Appendix B: Evidence Correlation Matrix

Evidence Source	Tool Used	Key Finding	Time Correlation
Chrome History	DB Browser	Download blocked	12:00:41 IST
MFT	MFTECmd	certutil execution	12:45:37 IST
Registry	Registry Explorer	CLSID hijacking	After 12:45:37
Event Logs	Manual	Defender detection	15:19:35 IST
File System	Autopsy	Wallpaper recovery	12:59:30 IST

Appendix C: Attack Chain MITRE ATT&CK Mapping

Tactic	Technique ID	Technique Name	Evidence
Initial Access	T1566.002	Phishing: Spearphishing Link	Chrome history, typosquatting domain

Execution	T1059.003	Command and Scripting: Windows Command Shell	certutil.exe usage
Persistence	T1547.001	Boot or Logon Autostart: Registry Run Keys	Startup VBScript
Privilege Escalation	T1068	Exploitation for Privilege Escalation	SeManageVolumePrivilege exploit
Defense Evasion	T1070.004	Indicator Removal: File Deletion	PrintConfig.dll deletion
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	certutil decode
Lateral Movement	T1021.001	Remote Services: Remote Desktop Protocol	RDP logs
Collection	T1005	Data from Local System	CFO proposal access

Appendix D: Anti-Forensic Techniques Identified

1. File System Manipulation

- **Secure Deletion:** PrintConfig.dll wiped preventing hash recovery
- **Timestamp Manipulation:** File times altered to blend with system files
- **Hidden Attributes:** VBScript set to hidden (12:56:11 IST)

2. Persistence Through Legitimate Mechanisms

- **DLL Search Order Hijacking:** Exploiting PrintNotify service
- **WBEM Directory Abuse:** tzres.dll in legitimate system directory
- **Startup Folder:** VBScript persistence via authorized autostart

3. Defense Evasion

- **LOLBIN Usage:** certutil.exe for download bypassing application controls
- **Browser Termination:** User shutdown to interrupt Safe Browsing blocking
- **Registry CLSID Hijacking:** Legitimate component compromise

Appendix E: Laboratory Learning Objectives

Technical Skills Developed:

1. **Browser Forensics:** Chrome History analysis, Safe Browsing interpretation

2. **Registry Analysis:** Persistence mechanism identification, CLSID investigation
3. **File System Forensics:** MFT timeline analysis, USN Journal parsing
4. **Evidence Correlation:** Multi-source timeline reconstruction
5. **Anti-Forensic Recognition:** File wiping, timestamp manipulation detection

Investigative Methodology:

1. Hypothesis-driven evidence collection
2. Chronological timeline reconstruction
3. Attack chain validation through multiple evidence sources
4. Professional documentation and reporting

Tool Proficiency:

- EZ Tools Suite (MFTECmd, Registry Explorer)
- SQLite database analysis (DB Browser)
- File carving and recovery (Autopsy)
- Command-line forensic utilities

Appendix F: Recommended Security Controls

Preventive Controls:

1. **Phishing Protection:** Advanced email filtering, user awareness training
2. **Application Whitelisting:** Restrict certutil and other LOLBINs
3. **Privilege Management:** Regular review of special privileges like SeManageVolumePrivilege
4. **Browser Security:** Enhanced Safe Browsing, download restrictions

Detective Controls:

1. **EDR Monitoring:** DLL search order hijacking detection
2. **File Integrity Monitoring:** Critical system directory changes
3. **User Behavior Analytics:** Anomalous RDP access patterns
4. **Registry Monitoring:** CLSID and service configuration changes

Response Controls:

1. **Incident Response Playbook:** RDP compromise response procedures
2. **Forensic Readiness:** Regular evidence collection testing
3. **Containment Strategies:** Network segmentation for remote workers
4. **Recovery Procedures:** System restoration from clean backups

APPENDIX G: DETAILED FORENSIC ARTIFACTS

1. Chrome History Database Analysis

Tables Examined:

- downloads: Primary table for download history
- urls: Browsing history and page visits
- visits: Timestamps and visit chain relationships

Key Fields Identified:

danger_type values:

0 = NOT_DANGEROUS

1 = DANGEROUS

2 = DANGEROUS_URL

3 = DANGEROUS_CONTENT

4 = UNCOMMON_CONTENT

5 = DANGEROUS_HOST

6 = POTENTIALLY_UNWANTED

7 = DANGEROUS_HOST (Found in evidence)

interrupt_reason values (partial):

0 = NONE

1 = FILE_FAILED

2 = FILE_ACCESS_DENIED

41 = USER_SHUTDOWN

Query Results for Malicious Download:

Time: 2025-05-28 12:00:41 IST

URL: http://freehackingtool.com/tools/PrintConfig.dll

Danger Type: 7 (DANGEROUS_HOST)

Interrupt Reason: 41 (USER_SHUTDOWN)

State: 2 (INTERRUPTED)

2. Windows Registry Artifacts

NTUSER.DAT Findings:

Path: Control Panel\Desktop

Key: Wallpaper

Value: C:/Users/Public/Pictures/gg.bmp

Last Modified: 2025-05-28 12:59:30

Path: Software\Microsoft\Windows\CurrentVersion\Run

Evidence: No malicious Run keys (cleanup detected)

SYSTEM Hive Findings:

Path: ControlSet001\Services\PrintNotify

Key: ImagePath

Value: %SystemRoot%\system32\svchost.exe -k LocalServiceNetworkRestricted

Path: ControlSet001\Services\PrintNotify\Parameters

Key: ServiceDll

Value: %SystemRoot%\system32\PrintNotify.dll

SOFTWARE Hive Findings:

Path: Classes\CLSID\{854A20FB-2D44-457D-992F-EF13785D2B51}

Last Write Time: 2025-05-28 12:48:00 (Post-compromise)

3. Master File Table (MFT) Timeline

Critical File Events:

2025-05-28 12:45:37 - C:\Windows\System32\spool\drivers\x64\3\PrintConfig.dll (Created)

2025-05-28 12:47:06 - C:\Windows\System32\PrintConfig.dll (Deleted)

2025-05-28 12:54:23 - C:\Windows\System32\wbem\tzres.dll (Created)

2025-05-28 12:56:11 - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\a.vbs (Attributes Modified)

2025-05-28 12:59:15 - C:\Users\Public\Pictures\gg.bmp (Created)

Process Execution Evidence:

2025-05-28 12:45:36 - C:\Windows\System32\certutil.exe (Last Accessed)

2025-05-28 12:48:00 - C:\Windows\System32\spool\drivers\x64\3\PrintConfig.dll (Last Accessed)

4. Windows Event Log Correlation

Security Log (Event ID 4624):

2025-05-27 11:59:57 - Logon Type 10 (RemoteInteractive) - Threat Actor

2025-05-28 15:04:41 - Logon Type 2 (Interactive) - Legitimate User

Windows Defender Logs:

Event ID: 1116 (Threat Detected)

Time: 2025-05-28 15:19:35

Threat: Trojan:Win64/Meterpreter.E

Path: C:\Windows\system32\spool\drivers\x64\3\PrintConfig.dll

FINAL OBSERVATIONS

The HackTheBox Sherlock "WorkFromHome" laboratory effectively simulates real-world DFIR challenges, including:

1. **Realistic Attack Chain:** Multi-stage compromise with clear objectives
2. **Anti-Forensic Techniques:** File wiping, timestamp manipulation
3. **Evidence Diversity:** Multiple artifact types requiring correlation
4. **Investigative Constraints:** Logical file extraction limitations

Laboratory Design Quality: Excellent - balanced difficulty, clear objectives, realistic artifacts

Educational Value: High - comprehensive DFIR skill development

Recommendation: Suitable for intermediate to advanced forensic analysts preparing for real-world investigations or certification exams.

DISCLAIMER

This report documents findings from the HackTheBox Sherlock "WorkFromHome" training laboratory. All analysis was conducted on provided training artifacts in a controlled lab environment. The information contained herein is for educational and training purposes only.

1. **No Real Data:** All systems, IP addresses, domains, and user information are part of a training simulation.
2. **Training Context:** Findings represent expected outcomes in a controlled educational environment.
3. **Methodology Demonstration:** Techniques shown are for forensic education, not actual incident response procedures.
4. **Legal Compliance:** This exercise complies with all applicable laws and ethical guidelines for forensic training.