INCS-712: Digital Forensics

Group Projects & Research Directions

Baljeet Malhotra, PhD

Group Projects - Research Directions

- ❑ Research Direction 1 – Digital Forensic Processes
- ❑ Research Direction 2 – Digital Forensic Tools
- ❑ Research Direction 3 – Digital Forensic Domains
- ❑ Research Direction 4 – Digital Forensic Industries/Sectors
- ❑ Research Direction 5 – Digital Forensics for Malicious Applications
- ❑ Research Direction 6 – Applications of AI and DS in Digital Forensic

Research Directions - Process & Tools

❑ Digital Forensic Investigation Process

- Digital Forensic Readiness
- Digital Forensic Examination and Analysis
- Quality and Legal Standards for Digital Forensics
- Global Justice and Judicial Systems for Digital Forensics

❑ Digital Forensic Tools

- Digital Forensic Identification and Acquisition Tools
- Digital Examination and Analysis Tools

❑ Dynamic Malware Analysis

- Android Malware Analysis
- IOS Malware Analysis

Research Directions - Domains

Network Forensics

- Tools and Techniques
- Case Studies / Research Challenges

Cloud Forensics

- Tools and Techniques
- Case Studies / Research Challenges

IoT Forensics

- Tools and Techniques
- Case Studies / Research Challenges

Research Directions - Domains

API Forensics

- Tools and Techniques
- Case Studies / Research Challenges

Mobile Forensics

- Tools and Techniques
- Case Studies / Research Challenges

Smartphone Forensics

- Tools and Techniques
- Case Studies / Research Challenges

Research Directions - Sectors

Digital Forensics in Criminal Investigations

- Criminal Pattern Detection using Data Mining
- Criminal Analysis and Prediction using Machine Learning
- Criminal Network Analysis using Machine Learning

Digital Forensics in Financial Investigations

- Financial Crime Detection

Digital Forensics for Social Media

- Social Media Forensics for Android Devices
- Social Media Forensics for IOS Devices
- Social Media Forensics for Windows Devices

Research Directions - AI & Data Science

AI-Driven Forensic Approaches

- Tools and Techniques
- Case Studies / Research Challenges

Big Data Forensics

- Tools and Techniques
- Case Studies / Research Challenges

Deepfake Forensics

- Tools and Techniques
- Case Studies / Research Challenges

INCS-712: Computer Forensics

Course Tools and Resources

Baljeet Malhotra, PhD

Digital Forensics Tools and Resources

Name	Description	Status	URL
Exiftools	Metadata analysis	Active	https://exiftool.org/
Hashmyfiles	Hash analysis	Dormant	https://github.com/forenipackages/hashmyfiles
TRID	Signature analysis	Active	https://mark0.net/soft-trid-e.html
Autopsy Forensic Analyzer	Data Carving, Analysis	Active	https://www.autopsy.com/
FTK Image, Arsenal Image Mounter, CAINE	Forensic Imaging & Mounting Image files	Active	https://www.caine-live.net/page11/page11.html
KAPE, Redline	Collection for Incident Response	Active	https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape
EricZimmerman Tools	Event Log Analysis	Active	https://ericzimmerman.github.io/
EricZimmerman Tools	Prefetch File Analysis	Active	https://ericzimmerman.github.io/
EricZimmerman Tools	MFT Parsing, timeline creation	Active	https://ericzimmerman.github.io/
Regripper	Registry Analysis	Dormant	https://github.com/keydet89/RegRipper3.0
EricZimmerman Tools	Jumplist, Link File	Active	https://ericzimmerman.github.io/
Timeline Explorer	Event Log Analysis	Active	https://ericzimmerman.github.io/
Volatility	Memory Forensics	Active	https://github.com/volatilityfoundation/volatility
Sysinternals	Live Forensics	Active	https://learn.microsoft.com/en-us/sysinternals/
MITRE ATT@CK	IR Framework	Active	https://attack.mitre.org/
WireShark	Packet analysis	Active	https://www.wireshark.org/

Digital Forensics Tools and Resources

Name	Description	Status	URL
EnCase Forensic	Collect/organize metadata from devices	Active	https://www.opentext.com/products/encase-forensic
ProDiscscover Forensics	Collect/organize metadata from devices	Active	https://prodiscover.com/
ArcSight Logger	Digital Forensic tool by MicroFocus	Dormant	https://www.microfocus.com/documentation/arcsight/logger-7.2.2
Netwitness Investigator	Malicious Activity Detection	Active	https://www.netwitness.com/contact-us/netwitness-investigator-freeware/
Change Auditor	Active Directory tracker by Quest	Active	https://www.quest.com/products/change-auditor-for-active-directory-queries/
Forensic Toolkit (FTK)	Digital Forensic tool by AccessData	Dormant	https://accessdata-ftk-imager.software.informer.com/3.1/
Physical Analyzer	Digital Forensic tools by Cellebrite	Active	https://cellebrite.com/en/physical-analyzer/
Lantern	Katana Forensics for iPhone/iPod/iPad	Dormant	http://www.mobileforensicscentral.com/mfc/products/lantern.asp?pg=d&prid=387&pid=
WinHex	Data Recovery and Digital Forensics by X-Ways AG.	Active	https://www.x-ways.net/winhex/
National Software Reference Library (NSRL)	Database of hashed files managed by NIST	Active	https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl
Malware-Feed	Repository that contains actual malware	Dormant	https://github.com/MalwareSamples/Malware-Feed
Cutter	An advanced FREE and open-source reverse-engineering platform	Active	https://cutter.re/

Digital Forensics Tools and Resources

Name	Description	Status	URL
PEiD	PEiD detects most common packers, cryptors and compilers for PE files.	Dormant	https://www.aldeid.com/wiki/PEiD
Immunity Debugger	A powerful tool to write exploits, analyze malware, and reverse engineer binary files.	Active	https://www.immunityinc.com/products/debugger/
Ghidra	Open source reverse engineering tool developed by the National Security Agency (NSA) of the United States	Active	https://github.com/NationalSecurityAgency/ghidra
x64dbg	Dynamic analysis and debugging of executables	Active	https://x64dbg.com/
OllyDbg	Assembler-level analyzing debugger for Windows, commonly used for dynamic analysis and debugging	Dormant	https://www.ollydbg.de/
xiosec/Reverse-engineering	Repository that contains list of Reverse Engineering tools	Active	https://github.com/xiosec/Reverse-engineering
stego-toolkit	Collection of steganography tools - helps with CTF challenges	Dormant	https://github.com/DominicBreuker/stego-toolkit
Burp Suite	scanning for API vulnerabilities, manipulating requests, and analyzing responses.	Active	https://portswigger.net/burp/communitydownload
API Discovery	API Forensics, API Security and API Fraud Analysis	Active	https://apidiscovery.teejlab.com/edsn/knowledgebase/