

COMP 5350 / 6350

Digital Forensics

Introduction to Digital Forensics

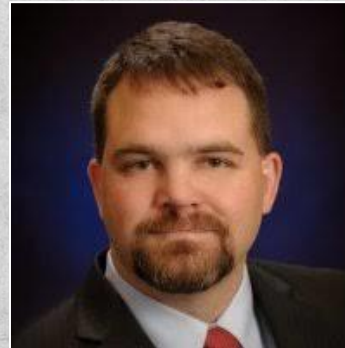


Agenda

- Instructor Introduction
- Administration
- Course Introduction
- History
- Digital Forensics Research Conference
- Legal Standards for Digital Forensics
- Digital Evidence Collection and Archiving
- Incident Response
- Forensics Testing Environment

Instructor Introduction

- Jason Cuneo
- West Point, 1998, B.S. Electrical Engineering
- U.S. Army, Infantry Officer, 1998 – 2004
- UAH, 2006, M.S. Electrical Engineering
- Auburn, Current, PhD Program, C.S. & Software Engineering
- Experience
 - ✓ Defensive Cyber Operations
 - ✓ Cyber Training
 - ✓ Advanced Networking
 - ✓ Cyber Exercises
 - ✓ System Vulnerability Assessments



Administration

- Course Dates:
 - ✓ 21 August – 4 December 2020
 - ✓ Friday, 12:00 – 2:30 pm
- Facilities
 - ✓ Shelby 1103
 - ✓ Emergency Exits
 - ✓ Restrooms
 - ✓ Breaks
- Digital Forensics Lab

Course Syllabus

Digital Forensics – COMP 5350 / 6350 / 6356 – Fall 2020

Course Description

Digital forensics is a division of forensic science that includes the investigation, collection, analysis, and recovery of digital artifacts in response to electronic attacks on organizational assets. During this course, each student will be introduced to the legal, ethical, and technical aspects of digital forensics and ultimately will develop critical thinking skills and rigorous analysis techniques to successfully perform a digital forensic investigation. Student understanding will be solidified through numerous hands-on projects in the collection, analysis, and recovery of digital artifacts.

Course Dates and Times

21 August – 4 December 2020

Every Friday, 12:00 – 2:30 pm, Shelby 1103

Contact Information

Name: Jason Cuneo

Email: jzc0105@auburn.edu

Phone: (334) 209-4762

Office: 2117 Shelby, ACRC Lab

Office Hours: Friday, 9:00 – 11:30 am, or by appointment

Course Description

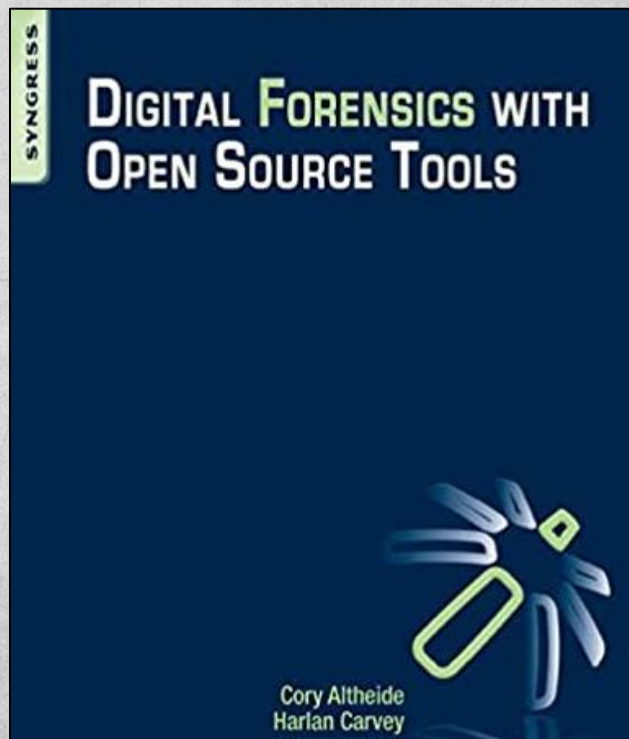
Digital forensics is a division of forensic science that includes the investigation, collection, analysis, and recovery of digital artifacts in response to electronic attacks on organizational assets. During this course, each student will be introduced to the legal, ethical, and technical aspects of digital forensics and ultimately will develop critical thinking skills and rigorous analysis techniques to successfully perform a digital forensic investigation. Student understanding will be solidified through numerous hands-on projects in the collection, analysis, and recovery of digital artifacts.

Learning Objectives

- Understand how digital forensics can be used to collect and analyze digital artifacts
- Identify and select digital forensic collection and analysis tools
- Understand differences in file systems and operating systems
- Apply sound digital forensics analysis techniques to identify system and network intrusions

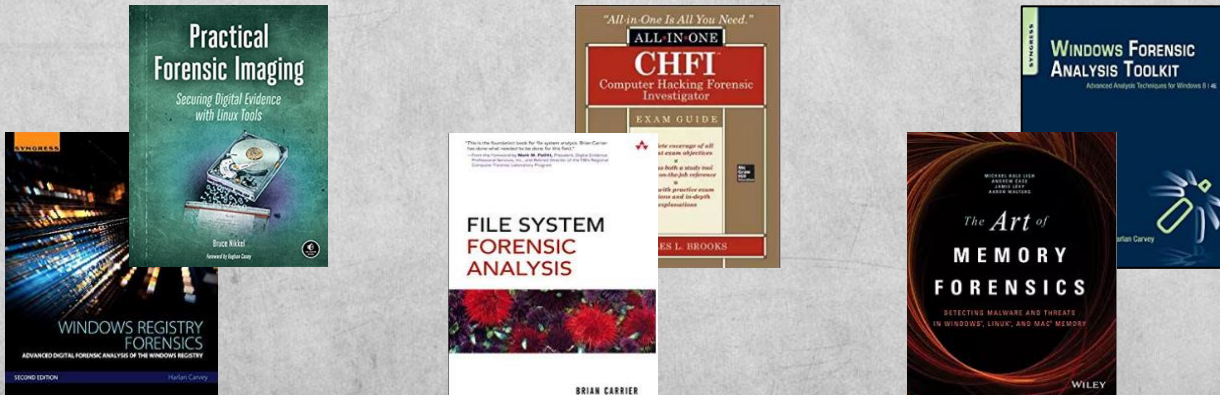
Course Text

Digital Forensics with Open Source Tools, 1st Edition, Altheide, Syngress Press, 2011



Course References

- Practical Forensic Imaging
- Windows Registry Forensics
- Computer Hacking Forensics Investigator
- Windows Forensic Analysis Toolkit
- Digital Forensics with Open Source Tools
- File System Forensics Analysis



Professional Certifications

- There are numerous professional certifications in digital forensics including:

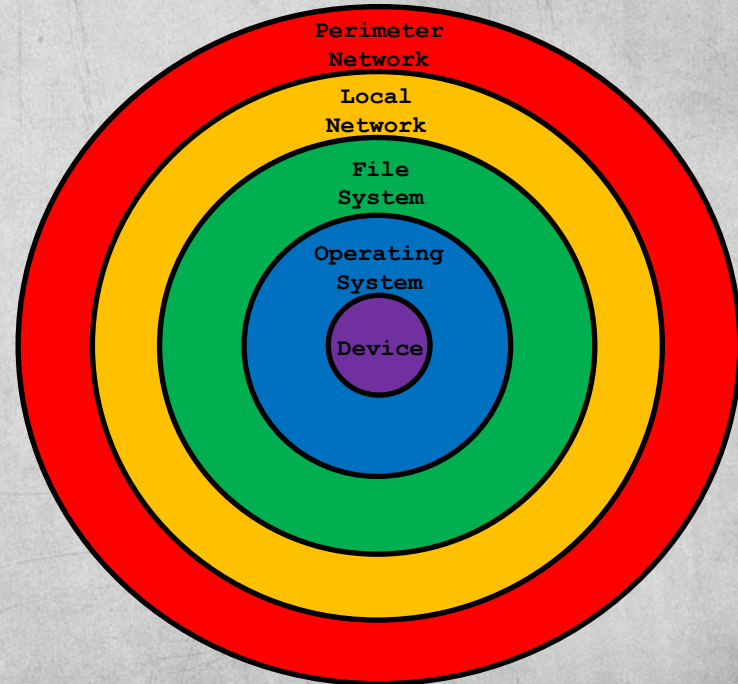
Certification	Certifying Organization
Certified Forensic Computer Examiner	IACIS
Computer Hacking Forensic Investigator	EC Council
Global Information Assurance Certified Forensic Analyst	SANS Institute
AccessData Certified Examiner - Forensic Tool Kit	AccessData
EnCase Certified Examiner - EnCase	OpenText

Additional Course Resources

- Additional resources are available from numerous organizations, developers, and security professionals relative to forensic collection and analysis:
 - ✓ NIST Digital Forensics
 - ✓ Linux Forensics Tools Repository - LiFTeR
 - ✓ Awesome Forensics Github Repo
 - ✓ Enron Email Dataset
 - ✓ Digital Corpora Disk Images
 - ✓ Memory Dumps

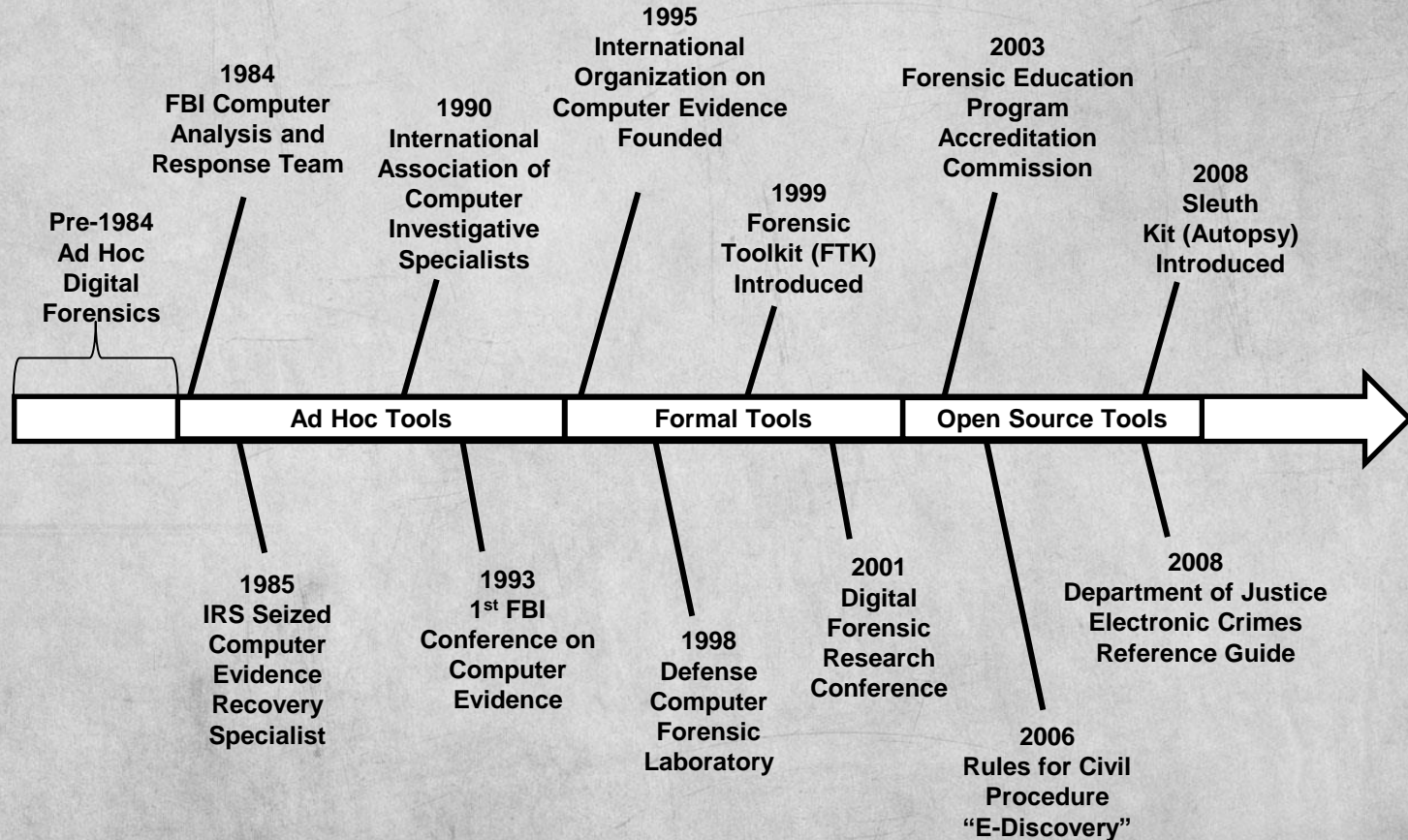
Course Overview

- In this course, we will learn how to conduct forensics collection and analysis from the inside to the outside
 - ✓ Device
 - ✓ Operating System
 - ✓ File System
 - ✓ Local Network
 - ✓ Perimeter Network



Digital Forensics History

Digital Forensics Timeline



Digital Forensics Research Conference

Digital Forensics Research Conference

- Just as traditional forensics analysis provides a rigorous process to deal with physical evidence, digital forensics is also developing consistent methods for its digital equivalent
- A Road Map for Digital Forensic Research was presented in 2001 at DFRWS
 - ✓ Digital Forensic Science Framework
 - ✓ Digital Evidence Trustworthiness
 - ✓ Detection and Recovery of Hidden Data
 - ✓ Network Forensics



A Road Map for Digital Forensic Research

By
Collective work of all DFRWS attendees

From the proceedings of
The Digital Forensic Research Conference
DFRWS 2001 USA
Utica, NY (Aug 7th - 8th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment.

As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

<http://dfrws.org>

Digital Forensics Usage

- Organizations that make use of digital forensics and associated frameworks include:
 - ✓ Law Enforcement (i.e. Local, State, Federal)
 - ✓ Military Information Warfare
 - ✓ Business and Industry
- Each of these organizations has different objectives when applying digital forensics techniques:
 - ✓ Law Enforcement – Prosecution
 - ✓ Military Information Warfare – Continuity of Operations
 - ✓ Business and Industry – Availability of Services

Digital Forensics Considerations

- Technical
 - ✓ Continuous Technology Improvement
 - ✓ Framework and Tool Development
 - ✓ Training
- Procedural
 - ✓ No standard analytical procedures
 - ✓ Different terminology
- Social
 - ✓ Privacy and Data Sharing
- Legal
 - ✓ State, Local, and Federal Governments

Digital Forensics Science Framework

- For any scientific discipline, there are several important considerations that must be met:
 - ✓ Theory
 - Agreed set of scientific principles
 - ✓ Process
 - Systematic observation, measurement, and testing
 - ✓ Elements of Practice
 - Applicable and agreed technologies and tools
 - ✓ Documentation
 - Professional literature
 - ✓ Usefulness
 - Proof that the discipline effectively meets a need

Digital Forensics Definition

The DFRC defined digital forensics as:

“The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations.”

Digital Forensics Investigative Process

Identification	Preservation	Collection	Examination	Analysis	Presentation
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation
Resolve Signature	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification
Anomalous Detection	Time Synchron.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation
Audit Analysis		Sampling	Hidden Data Extraction	Link	
Etc.		Data Reduction		Spacial	
		Recovery Techniques			

6-Step Process

Identify
 Preserve
 Collect
 Examine
 Analyze
 Present

Digital Forensics

Investigative Process Questions

Identify – Preserve – Collect – Examine – Analyze – Present

- 1) Imaging a disk**
- 2) Building timelines with packet captures**
- 3) Securing a laptop for forensic analysis**
- 4) Correlating system intrusions with data mining**
- 5) Providing subject matter expertise for a trial**
- 6) Finding hidden data on a disk partition**

Digital Forensics Investigative Process Questions

Identify – Preserve – Collect – Examine – Analyze – Present

- 1) Imaging a disk – Preservation**
- 2) Building timelines with packet captures – Analysis**
- 3) Securing a laptop for forensic analysis – Preservation**
- 4) Correlating system intrusions with data mining – Analysis**
- 5) Providing subject matter expertise for a trial – Presentation**
- 6) Finding hidden data on a disk partition – Examination**

Digital Evidence Trustworthiness

- Since digital media and data can be manipulated, a process is necessary to correctly collect and store digital artifacts
- Some methods to ensure data trustworthiness include:
 - ✓ Working from an exact copy of original data
 - ✓ Preserving data integrity
 - Image and File Hashes
 - Collection Time and Time Offsets
 - ✓ Employing cryptography
 - Digital signatures – Asymmetric
 - Encryption – Symmetric and Asymmetric
 - ✓ Understand application metadata
 - ✓ Apply corroborating evidence

Hidden Data Methods

- Digital forensic analysts should understand likely hiding methods and locations used to obscure and conceal data
- The DFRC identified 10 data hiding methods to conceal data
- Prior to analyzing media, we must detect data hiding methods

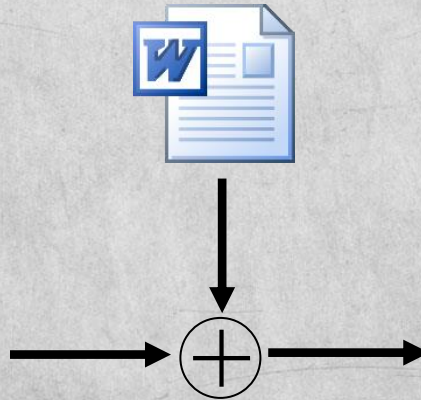
Graphics	Signals	Applications	Disk Geomerty	File Systems	Comm Structures	Solid State	Data Structures	OS & Programming	Non-Digital
Least Significant Bit	Altered Compression Algorithms	Compound Doc formats	Marked Bad Clusters	Distributed Systems	Reserved Packet offsets	BIOS	Heap Space	Virus-like expressiosn	Perception
Audio	Stego	metadata - reserved structures	Maintenance Track	RAM Slack	Email Spam	CMOS		Rootkits altering system calls	Filenames
Video	timing channels	File Slack	Extra tracks	Modified Dir Entries	Protocols	RAM		System Libraries	Plain sight
Imagery	sequencing		Hidden partitions	Unallocated Space				DLL's	
Stego				Boot Sector					

Hidden Data Methods

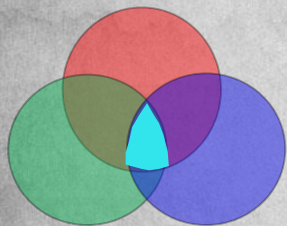
- **Graphics**
 - ✓ **LSB Stego**
- **Applications**
 - ✓ **File Slack**
- **Disk Geometry**
 - ✓ **Hidden Partitions**
- **File Systems**
 - ✓ **RAM Slack**
 - ✓ **Unallocated Space**
 - ✓ **Boot Sector**
- **Communication Structures**
 - ✓ **Reserved Packet Offsets**
 - ✓ **Protocols**
- **Solid State**
 - ✓ **BIOS - UEFI**
 - ✓ **RAM**
- **Data Structures**
 - ✓ **Stack & Heap Space**
- **Operating System**
 - ✓ **System Libraries**
 - ✓ **Dynamic Linked Libraries**

Steganography

- Hiding data or media in other media
 - ✓ “Security through obscurity”
- Examples of steganography tools:
 - ✓ Steghide
 - ✓ Xiao



LSB Steganography



#32E4EC



#320000



#00E400



#0000EC



#32E4EC → 1100101110010011101100

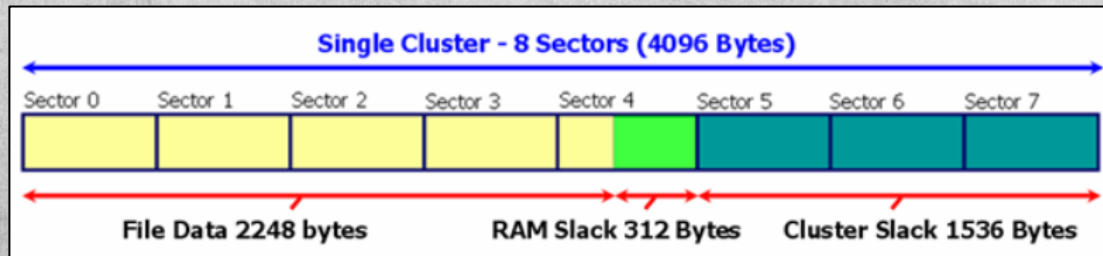


1100101110010011101101 → #32E4ED



File Slack

- Another data hiding technique uses file slack which is the remaining sector of a cluster and requires understanding of:
 - ✓ Disk Geometry
 - Sectors – The smallest addressable data element
 - 512 bytes → 4 KB
 - ✓ Operating Systems – File Systems
 - Clusters – The smallest addressable data element for a file system
 - 8 sectors



Hidden Partitions


- A partition is a unique region on storage media that an operating system can manage
- Hidden partitions are generally used to restore default system settings, but can be manipulated to store data

```
DISKPART> list volume
```

Volume ###	Ltr	Label	Fs	Type	Size	Status	Info
Volume 0	D	DATA	NTFS	Partition	931 GB	Healthy	
Volume 1	C	OS	NTFS	Partition	105 GB	Healthy	Boot
Volume 2		WINRETOOLS	NTFS	Partition	476 MB	Healthy	
Volume 3		Image	NTFS	Partition	11 GB	Healthy	
Volume 4		DELLSUPPORT	NTFS	Partition	1109 MB	Healthy	
Volume 5		ESP	FAT32	Partition	650 MB	Healthy	System

Unallocated Space

- Operating systems and their associated file systems allocate storage based on different methods
- Allocated space
 - Contains data
 - Marked so that it cannot be overwritten
- Unallocated space
 - May or may not contain data
 - Marked so that it can be overwritten

 Disk 1 Basic 119.12 GB Online						
	650 MB Healthy (EFI System Part)	OS (C:) 105.13 GB NTFS Healthy (Boot, Page File, Crash Dump, Primar	WINRETOOLS 476 MB NTFS Healthy (OEM Partitior	Image 11.79 GB NTFS Healthy (OEM Partition)	DELLSUPPORT 1.08 GB NTFS Healthy (OEM Partition)	10 MB Unalloc

Communication Protocols

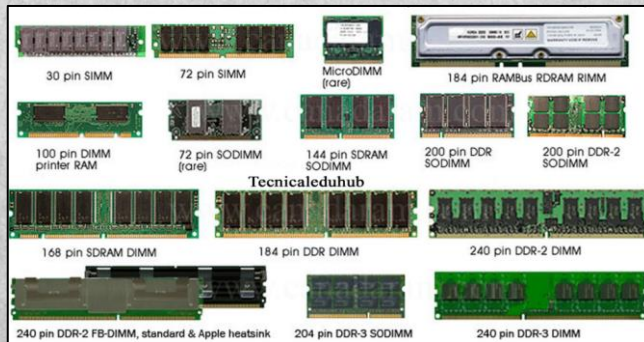
- Request for Comments (RFC) specify the technical parameters of communication protocols
- Digital forensic analysis will be used to identify potential covert channels and hidden data each OSI layer:
 - ✓ Application
 - ✓ Presentation
 - ✓ Session
 - ✓ Transport
 - ✓ Network
 - ✓ Data Link
 - ✓ Physical

System Boot

- System boot methods can be manipulated to hide data
 - ✓ Basic Input / Output System (BIOS)
 - Master Boot Record (MBR)
 - Single boot sector
 - 512-byte disk sectors
 - 4 partition limit
 - 2 TB maximum addressable space
 - ✓ Unified Extensible Firmware Interface (UEFI)
 - Globally Unique Identifier (GUID) Partition Table (GPT)
 - 512 bytes → 4 KB disk sectors
 - 128 partition limit (OS Dependent)
 - 8ZB → 64ZB maximum addressable space

Random Access Memory

- Data can also be hidden in Random Access Memory (RAM)
 - ✓ Static RAM (SRAM)
 - ✓ Dynamic RAM (DRAM)
 - ✓ Synchronous Dynamic RAM (SDRAM)
 - ✓ Single Data Rate Synchronous Dynamic RAM (SDR SDRAM)
 - ✓ Double Data Rate Synchronous Dynamic RAM
 - DDR SDRAM, DDR2, DDR3, DDR4



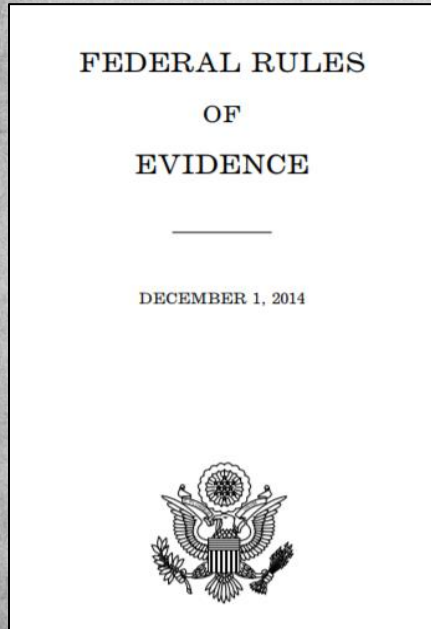
Digital Forensics Legal Considerations

Digital Evidence

- The U.S. Department of Justice published a reference guide for first responders relative to electronic crimes in 2008
- It specifies 14 crime categories and 60 different types of digital evidence
- Examples of digital evidence include:
 - Video cameras
 - Audio recorders
 - Sim card reader
 - Video game consoles



Federal Rules of Evidence



- Enacted by Public Law 93–595 and approved January 2, 1975
- FRE Articles include:
 - ✓ Article VI – Witnesses
 - ✓ Article VII – Opinions and Expert Testimony
 - ✓ Article VIII – Hearsay
 - ✓ Article IX – Authentication and Identification
 - ✓ Article X – Contents of Writings, Recordings, and Photographs

Best Evidence

- When considering different digital data sources, it is important to understand the distinction between evidence types defined by the Federal Rules of Evidence:
- Best Evidence – FRE 1001
 - ✓ “For electronically stored information, “original” means any printout — or other output readable by sight — if it accurately reflects the information.”
 - ✓ Actual memory vs. memory dump

Locard's Exchange Principle

- Locard's Exchange Principle “holds that the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence.”¹
- The concept that “every contact leaves a trace” holds both in physical and electronic forensics



Computer Generated vs. Computer Stored Records

- Computer Generated
 - ✓ Data generated by a computing system or program
- Computer Stored
 - ✓ Records or documents generated by a user
- Depending on the type of data generated determines whether it is considered hearsay in a court of law:
 - ✓ Computer generated data is considered direct evidence - FRE 803(6)
 - ✓ Computer stored data is considered hearsay unless corroborated

Computer Generated vs. Computer Stored Records

➤ Identify which digital artifacts are computer generated and which are computer stored:

- ✓ Email
- ✓ Chat Session
- ✓ Security Logs
- ✓ Packet Capture
- ✓ Cron Job
- ✓ Intrusion Detection Alerts

Computer Generated vs. Computer Stored Records

➤ Identify which digital artifacts are computer generated and which are computer stored:

- ✓ Email – Computer Stored
- ✓ Chat Session – Computer Stored
- ✓ Security Logs – Computer Generated
- ✓ Packet Capture – Computer Generated
- ✓ Cron Job – Computer Generated
- ✓ Intrusion Detection Alerts – Computer Generated

Digital Evidence Collection and Archiving

Guidelines for Evidence Collection and Archiving

- Request for Comment (RFC) 3227 specifies best practices for digital evidence collection and storage
 - ✓ Guiding Principles during Evidence Collection
 - ✓ The Collection Procedure
 - ✓ The Archiving Procedure
 - ✓ Tools
 - ✓ References

Network Working Group
Request for Comments: 3227
BCP: 55
Category: Best Current Practice

D. Brezinski
In-Q-Tel
T. Killalea
neart.org
February 2002

Guidelines for Evidence Collection and Archiving

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

A "security incident" as defined in the "Internet Security Glossary", RFC 2828, is a security-relevant system event in which the system's security policy is disobeyed or otherwise breached. The purpose of this document is to provide System Administrators with guidelines on the collection and archiving of evidence relevant to such a security incident.

If evidence collection is done correctly, it is much more useful in apprehending the attacker, and stands a much greater chance of being admissible in the event of a prosecution.

Order of Volatility

- RFC 3227 specifies that data collection should be conducted on the most volatile storage elements first
 - ✓ CPU Cache and Registers
 - ✓ Routing Tables / ARP Cache / Process Tables / Kernel Statistic / RAM
 - ✓ Temporary File Systems / Swap Space
 - ✓ Remote Logging / System Monitoring Data
 - ✓ Physical Configuration / Network Topology
 - ✓ Archival Media

Legal Aspects of Digital Evidence Collection

- RFC 3227 specifies 5 legal considerations when presenting digital evidence:
 - ✓ Admissible: Must conform to legal rules
 - ✓ Authentic: Positively tie evidence to an incident
 - ✓ Complete: Must tell a complete story
 - ✓ Reliable: The evidence collection and storage process can not cast doubt on authenticity and veracity
 - ✓ Believable: Must be believable and understandable by a court



Digital Evidence Collection Process

- Capture System Image
 - ✓ Take forensically sound disk images
 - ✓ Determine the image and copy types
 - Live or Dead Image
 - Block or Bit-By-Bit Copy
- Document Network Traffic and Logs
 - ✓ Full network captures and system logs
 - ✓ Record MAC times (Modified, Accessed, Created)



Digital Evidence Collection Process

- Record Time Offset
 - ✓ Determine time offset between machine time and actual time
- Take Artifact Hashes
 - ✓ Hash drive images, databases, and individual files help to ensure that no modification of the data occurs during analysis or during transport
 - ✓ Determine which hash algorithm will be used during the collection process
 - MD5, SHA-1, SHA-2, SHA-3

Write Blockers

- Write blocks are essential to the collection process and include both hardware and software variants
- There are several NIST recommended write blocker recommendations
 - https://www.cfft.nist.gov/hardware_write_block.htm
- Software write blockers are less reliable



Digital Forensics and Incident Response

Threat Actors

- Expanding on intentional threats, we will find attackers fall into one or more of the following categories:
 - ✓ Advanced Persistent Threat (APT)
 - Nation State with significant financial and computing resources
 - ✓ Criminals
 - Financially driven
 - ✓ Hacktivist
 - Politically driven



Threat Actors

- Additional threat actor categories include:
 - ✓ Disgruntled Employees
 - Revenge driven
 - ✓ Script Kiddies
 - Limited technical capabilities
 - ✓ Hackers
 - Black Hat



Incident Response

- Digital forensics will be part of a comprehensive organizational incident handling and response policy
- Incidents are any activities launched against organizational resources that attempt to gain unauthorized access, violate security policy, or compromise system resources
- An effectively incident response will include:
 - ✓ Definitions of computer events vs. computer incidents
 - ✓ Incident categories
 - ✓ How incidents are forensically analyzed
 - ✓ How incidents are reported

Computer Security Events

- A computer security event is any detectable occurrence in a system or network
 - ✓ Users querying data from a database
 - ✓ A web server receiving responding to a web request
 - ✓ A user emailing a file
 - ✓ A router routing traffic
- None of these events result in a negative impact on organizational resources

Computer Security Incidents

- Any computer security event that negatively effects organizational resources and degrades normal operations are further categorized as adverse events and result in a security incident
- A computer security incident then is “a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices”¹
 - Denial of service against a web server
 - Unauthorized access to a user account
 - Downloading and installation of malware
 - Sensitive data exfiltration

Computer Security Incident Categories

- Numerous organizations define security incidents and the methods that should be employed to properly respond:
 - ✓ Department of Defense (DoD)
 - ✓ National Institute for Standards and Technology (NIST)

DoD Incident Categories

Category	Definition
CAT 0	Exercise - Testing
CAT 1	Root Level Access
CAT 2	User Level Access
CAT 3	Unsuccessful Access Attempt
CAT 4	Denial of Service
CAT 5	Improper Usage - Misconfiguration
CAT 6	Scan
CAT 7	Malicious Code
CAT 8	Investigation
CAT 9	Explained Anomaly

NIST Incident Categories*

Category	Definition
CAT 0	Exercise - Testing
CAT 1	Unauthorized Access
CAT 2	Denial of Service
CAT 3	Malicious Code
CAT 4	Improper Usage
CAT 5	Scan - Attempted Access
CAT 6	Investigation

Incident Categorization

- Categorize each security incident scenario
 - ✓ A forensic disk analysis results in positive identification of a rootkit
 - ✓ Network traffic artifacts shows multiple port scans
 - ✓ Security log analysis shows successful escalation to and administrative level system access
 - ✓ A forensic analysis of a Windows registry shows multiple violations of software installation policy

Incident Categorization

- Categorize each security incident scenario
 - ✓ A forensic disk analysis results in positive identification of a rootkit – 3
 - ✓ Network traffic artifacts shows multiple port scans – 5
 - ✓ Security log analysis shows successful escalation to and administrative level system access – 1
 - ✓ A forensic analysis of a Windows registry shows multiple violations of software installation policy – 4

Computer Incident Response Policy

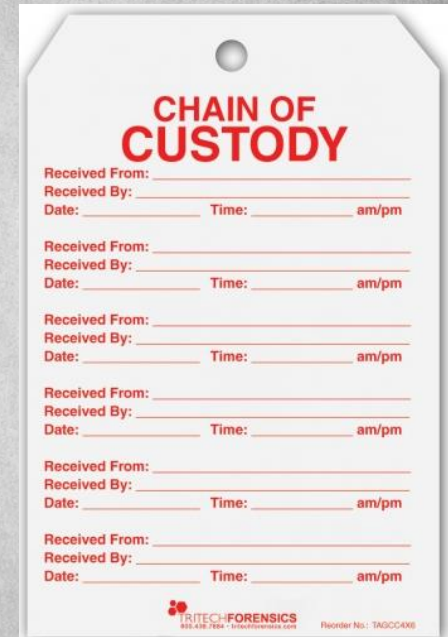
- Organizations should have an incident response policy that includes digital forensics collection and analysis capabilities
 - ✓ Incident Identification
 - Tools and procedures to detect potential incidents
 - ✓ Incident Investigation
 - Trained personnel in incident investigation and digital forensics collection and analysis process
 - ✓ Incident Damage Repair
 - A process to remediate incident damage

Computer Incident Response Policy

- The incident response policy should also include:
 - ✓ Documenting Organizational Response
 - Documenting all process, security, and administrative activities conducted during the response
 - ✓ Updating Incident Response Procedures
 - Integrate lessons learned into the process to make the next even more efficient

Chain of Custody

- To ensure proper control of electronic evidence an effective chain of custody policy should be implemented to ensure data integrity
 - ✓ Documenting artifacts collected
 - ✓ Identifying the collecting agent
 - ✓ Segregating items in secured facilities
 - ✓ Calculating artifact hashes
 - ✓ Securely transporting evidence
 - ✓ Conduct proper hand-off of evidence



CHAIN OF CUSTODY

Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

TRITECH FORENSICS
800.438.7884 • tritechforensics.com
Form No.: TAQCC408

Forensics Testing Environment Configuration

SIFT Installation Guide

- A full installation guide has been provided in Canvas to configure the SANS SIFT Forensics Analysis VM
 - ✓ Mac, Linux, and Windows

Download Ubuntu 18.04

Download the most current version of Ubuntu 18.04:

<https://releases.ubuntu.com/18.04/>

If you are working from the command line you can also use:

wget <https://releases.ubuntu.com/18.04/ubuntu-18.04.4-desktop-amd64.iso>

Note: Make sure to check your architecture to select the correct ISO

Download and Install VMWare Workstation or Fusion Pro

Auburn students can download VMWare Workstation and Fusion Pro from OnTheHub:

https://e5.onthehub.com/WebStore/Welcome.aspx?ws=b358730a-e638-de11-b696-0030485a8df0&utm_medium=school-finder&utm_campaign=school-finder&utm_source=Auburn%20University%20-%20Campus

Search for “VMWare” and find the software appropriate for your system. Once downloaded, follow the guided installation process.

References

- <https://kb.digital-detective.net/display/BLADE1/File+System+Data+Recovery>