

# Introduction to Digital Forensics and Incident Response (DFIR)

Omar Santos

 Follow @santosomar

# Agenda

- Introduction to the Incident Response Process
- Building an Incident Response Team
- The Incident Response Plan
- Incident Response Playbooks
- Digital Forensics Fundamentals
- Network and Host-based Evidence Collection and Handling

## POLL QUESTION 1

What is your level of familiarity with Digital Forensics and Incident Response?

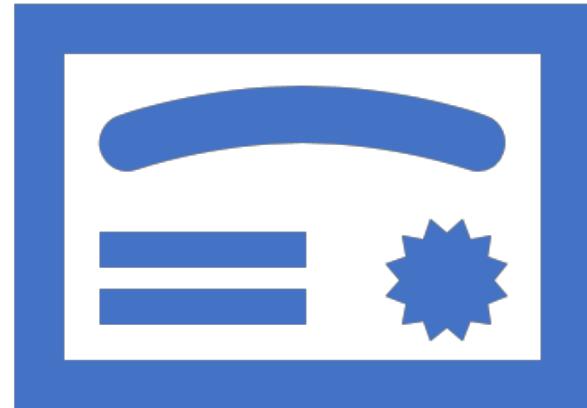
1. Beginner (less than 1 year of experience).
2. Intermediate (2-3 years of experience)
3. Expert (considerable experience).

## POLL QUESTION 2

Why are you interested in this course?

1. Just curious and want to learn more about DFIR.
2. I am preparing for a cybersecurity certification.
3. My job is DFIR.

# DFIR Related Certifications





DEEPER KNOWLEDGE.  
ADVANCED SECURITY.

## Interactive NICE Framework Mapping

SANS and GIAC Certifications has partnered with the National Security Workforce to place over 35 cyber security courses and corresponding GIAC certifications within an easy to read framework (commonly known as the NICE Framework.) The interactive framework below will help you identify the SANS courses and certifications you need to advance your career as a Federal Employee.

Many of the courses and certifications found on the NICE Framework are DoDD 8140 (DoDD 8570) compliant. Visit the [DoDD 8140](#) resource page for the full list of associated GIAC Certifications.

[How to use the NICE Framework Mapping](#)

[Download the Full NICE Mapping PDF](#)

Hover over the area of interest on the NICE Framework to get started.



GIAC Certified Incident Handler x +

https://www.giac.org/certification/certified-incident-handler-gcih

Login  +Q

GIAC CERTIFICATIONS

Certifications | Exams | Certified Professionals | Programs | Resources | About

## Security Certification: GCIH

### GIAC Certified Incident Handler (GCIH)

[View Professionals](#)

#### Description

Incident handlers manage security incidents by understanding common attack techniques, vectors and tools as well as defending against and/or responding to such attacks when they occur. The GCIH certification focuses on detecting, responding, and resolving computer security incidents and covers the following security techniques:

- The steps of the incident handling process
- Detecting malicious applications and network activity
- Common attack techniques that compromise hosts
- Detecting and analyzing system and network vulnerabilities
- Continuous process improvement by discovering the root causes of incidents

\*No specific training is required for any GIAC certification. There are many sources of information available regarding the certification objectives' knowledge areas. Practical experience is an option; there are also numerous books on the market covering Computer Information Security. Another option is any relevant courses from training providers, including SANS.\*

#### Requirements

- 1 proctored exam
- 150 questions

Get Certified ▾

Penetration Testing

GCIH

GPEN

GWAPT

GXPN

GMOB

GAWN

GPYC

Digital Forensics Certification X Omar

https://www.isc2.org/Certifications/CCFP

REGISTER FOR EXAM SIGN IN 

**(ISC)<sup>2</sup>** ABOUT CERTIFICATIONS EDUCATION & TRAINING MEMBERS NEWS & EVENTS ADVOCACY COMMUNITY

 *The CCFP will be designated an inactive credential August 21, 2020. The credential will remain a recognized (ISC)<sup>2</sup> certification until that date.*

 Certified Cyber Forensics Professional

The CCFP certification indicates expertise in forensics techniques and procedures, standards of practice, and legal and ethical principles to assure accurate, complete, and reliable digital evidence admissible in a court of law. It also indicates the ability to apply forensics to other information security disciplines, such as e-discovery, malware analysis, or incident response.

CCFP addresses more experienced cyber forensics professionals who already have the proficiency and perspective to effectively apply their cyber forensics expertise to a variety of challenges. In fact, many new CCFP professionals likely hold one or more other digital forensics certifications.

Given the varied applications of cyber forensics, CCFP professionals can come from an array of corporate, legal, law enforcement, and government occupations, including:

- Digital forensic examiners in law enforcement to support criminal investigations
- Cybercrime and cybersecurity professionals working in the public or private sectors
- Computer forensic engineers & managers working in corporate information security
- Digital forensic and e-discovery consultants focused on litigation support
- Cyber intelligence analysts working for defense/intelligence agencies
- Computer forensic consultants working for management or specialty consulting firms.

 Start Your Journey to Membership Today  
Pick the Certification that's Right for You 

**EC-Council**



<https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi>

By browsing this site, you are agreeing to our cookie policy. [More Information](#)

# CERTIFICATIONS

## Sharpen Your Competitive Edge

Our certification programs are led by the industry pioneers that help advance the careers of over 60,000 expert forensic investigators who consider EnCase technology as the gold standard in the industry.

### Choose Your Certification Path:

CFSR™  
CertificationEnCE®  
CertificationEnCEP®  
Certification

## CFSR™ Certification Program

Cyber security professionals who want to advance their careers are making it a top priority to get certified with cutting-edge techniques in real-world, digital forensic applications. The Certified Forensic Security Responder(CFSR™) will equip you with the breadth and depth of knowledge that you need to become a highly sought-after cyber security forensics expert.

**Prerequisites:**

Host Intrusion Methodology and Investigation + Incident Investigation Classroom / vClass or 12 Months of Qualified Work Experience

[Get Started »](#)[Apply »](#)[Renew »](#)

## EnCE® Certification Program

The EnCase® Certified Examiner(EnCE®) program certifies both public and private

# Introduction to the Incident Response Process

# Incident Response ISO and NIST References

- ISO- Section 16 of ISO 27002:2013:
  - Information Security Incident Management focuses on ensuring a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.
- NIST - Corresponding NIST guidance is provided in the following documents:
  - SP 800-61 Revision 2: "Computer Security Incident Handling Guide"
  - SP 800-83 Revision 1: "Guide to Malware Incident Prevention and Handling"
  - SP 800-86: "Guide to Integrating Forensic Techniques into Incident Response"

# INTRODUCTION TO INCIDENT RESPONSE

Computer security incident response is a critical component of information technology (IT) programs.

The incident response process and incident handling activities can be very complex.

One of the best resources available is NIST Special Publication 800-61:



Special Publication 800-61  
Revision 2

---

## **Computer Security Incident Handling Guide**

---

### **Recommendations of the National Institute of Standards and Technology**

---

Paul Cichonski  
Tom Millar  
Tim Grance  
Karen Scarfone

# What is an Event?

Definition from NIST Special Publication 800-61

“An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.”

Additional Reading: <http://h4cker.org/dfir/irt1.html>

# What is an Incident?

Definition from NIST Special Publication 800-61

“A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.”

Additional Reading: <http://h4cker.org/dfir/irt1.html>

## Examples of Incidents

Incident 1	Attacker compromises point-of-sale system and steals credit card information.
Incident 2	Attacker sends crafted packet to router and causes a crash and denial-of-service condition.
Incident 3	Ransomware is installed in critical server and all files are encrypted by the attacker.
Incident 4	User clicks on link sent in a phishing email and malware is installed on his machine.

Additional Reading: <http://h4cker.org/dfir/it1.html>

# Other Boring Definitions

---

For your reference only...

False positive is a broad term that describes a situation in which a security device triggers an alarm but there is no malicious activity or an actual attack taking place.

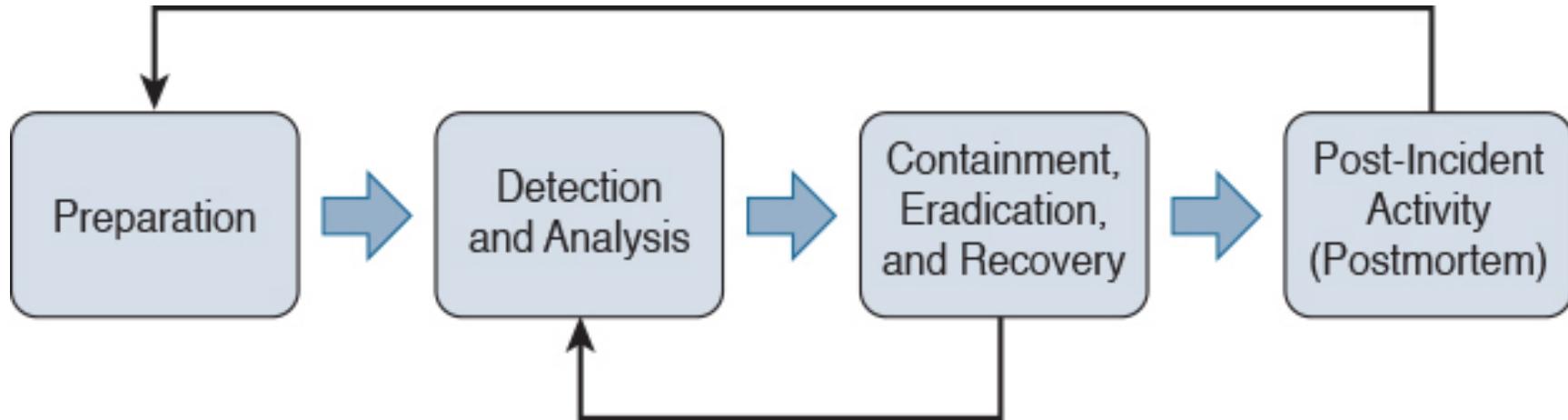
In other words, false positives are “false alarms,” and they are also called “benign triggers.”

False positives are problematic because by triggering unjustified alerts, they diminish the value and urgency of real alerts. If you have too many false positives to investigate, it becomes an operational nightmare, and you most definitely will overlook real security events.

False negatives: the term used to describe a network intrusion device's inability to detect true security events under certain circumstances in other words, a malicious activity that is not detected by the security device.

True positive: a successful identification of a security attack or a malicious event.

True negative: when the intrusion detection device identifies an activity as acceptable behavior and the activity is actually acceptable.



The Incident Response Process  
(reference NIST 800-61r2)

VERIS

The Vocabulary for  
Event Recording and  
Incident Sharing

vz-risk/VCDB: VERIS Community Database

This repository Search Pull requests Issues Marketplace Explore

vz-risk / VCDB

Code Issues 5,000+ Pull requests 3 Projects 0 Wiki Insights

VERIS Community Database

429 commits 4 branches 4 releases 10 contributors

Branch: master New pull request Create new file Upload files Find file Clone or download

Gabriel Bassett updated data to match updated json Latest commit e4e8844 on Mar 15

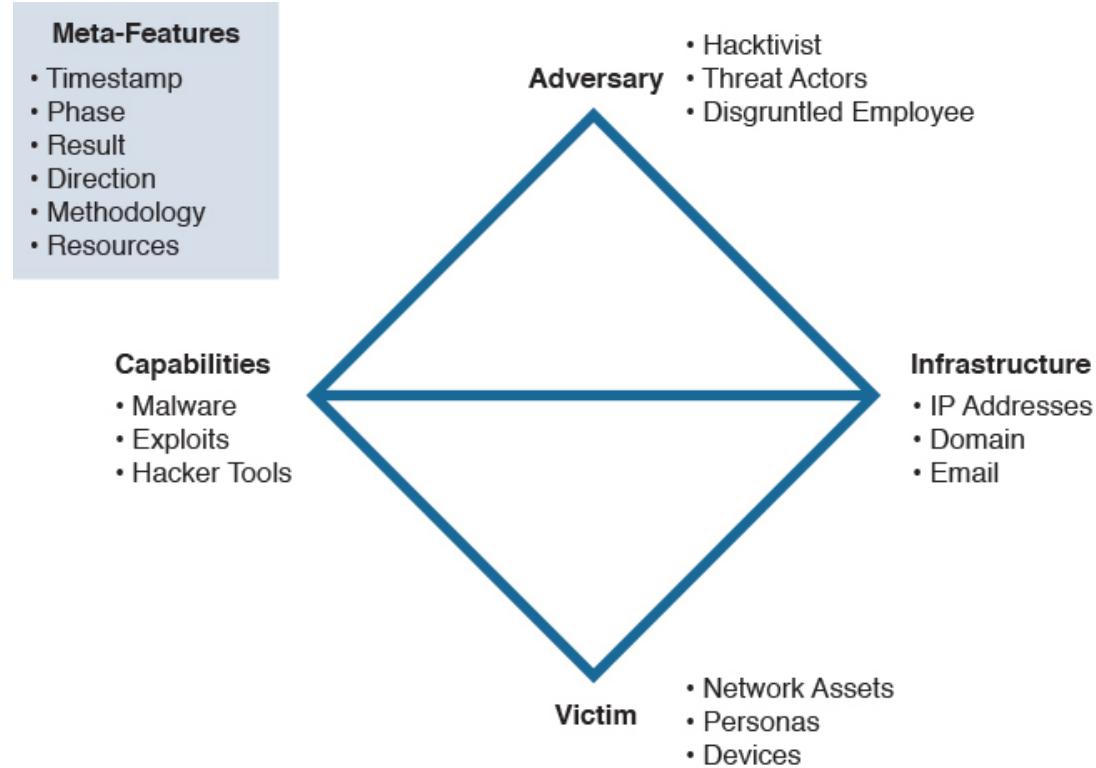
bin	updated the data files to contain all the nit-picky stuff I just fixed	4 months ago
data	updated data to match updated json	2 months ago
figure	Minor updates to readme	4 months ago
tools	Small changes	2 years ago
.gitignore	changed character in front of webskimmer breach directory. Added scrip...	7 months ago
LICENSE.txt	adds license file.	4 years ago
README.Rmd	updated Readme, removing ref to code.	4 years ago
README.md	Minor updates to readme	4 months ago
campaigns.md	Update campaigns.md	3 years ago
vcdb-enum.json	added 'unk' to event_chain object values	3 months ago
vcdb-keynames-real.txt	minor fixes to version 1.3.2	6 months ago
vcdb-labels.json	added 'unk' to event_chain object values	3 months ago
vcdb-merged.json	added 'unk' to event_chain object values	3 months ago
vcdb.json	updated schema to allow duplicates in event_chain	3 months ago
vcdb_diff-labels.json	added 'unk' to event_chain object values	3 months ago
vcdb_diff.json	updated schema to allow duplicates in event_chain	3 months ago

README.md

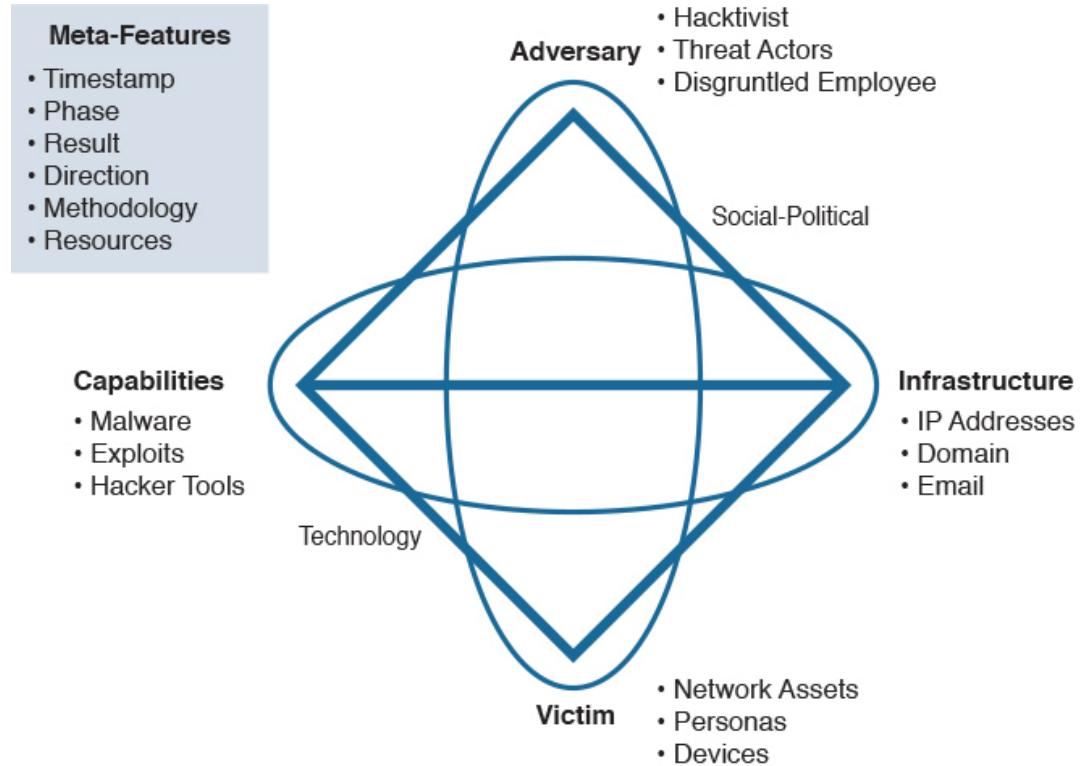
## The VERIS Community Database

Information sharing is a complex and challenging undertaking. If done correctly, everyone involved benefits from the collective intelligence. If done poorly, it may mislead participants or create a learning opportunity for our adversaries. The Verizon RISK Team supports and participates in a variety of information sharing initiatives and research efforts. We continue to drive the publication of the Verizon Data Breach Investigations Report (DBIR) annually, where we have an

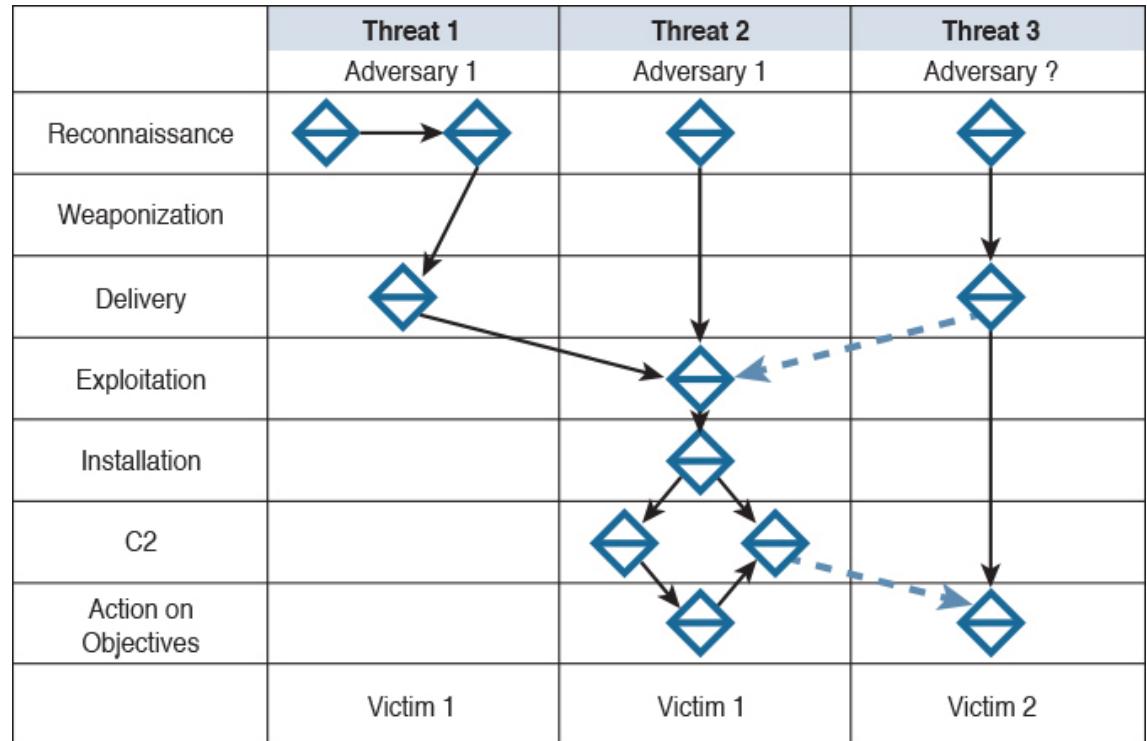
# The Diamond Model of Intrusion



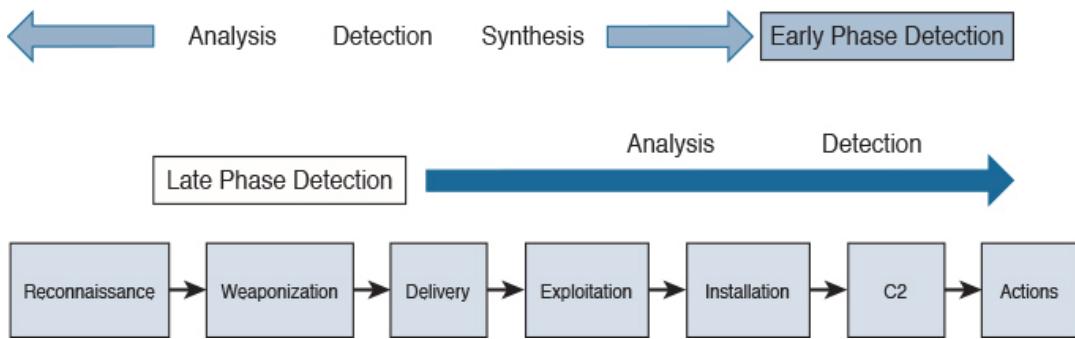
# The Diamond Model of Intrusion



# The Diamond Model of Intrusion



# Early and Late Detection in the Kill Chain



# Incident Response Teams

- Computer Security Incident Response Team (CSIRT)
- Product Security Incident Response Team (PSIRT)
- National CSIRTs and Computer Emergency Response Teams (CERTs)
- Coordination center
- Incident response teams of security vendors and managed security service providers (MSSP)

# FIRST

The screenshot shows the official website for FIRST (Forum of Incident Response and Security Teams). The header features the FIRST logo with the tagline "Improving Security Together". A navigation bar at the top includes links for About FIRST, Membership, Initiatives, Standards & Publications, Events, Education, and Blog. The main content area has a green header "About FIRST". Below it is a sidebar with a list of links: Mission Statement, History, Organization, FIRST Policies, Partners & Affiliates, Newsroom, Procurement, and Contact. To the right, the main article discusses the history of FIRST, mentioning its creation in 1989 after the Internet worm, and its mission to handle security vulnerabilities and incidents. It also highlights the variety of member teams from government, commercial, and academic sectors. At the bottom left, there's a map of the world with green shading over Europe and parts of Asia, and a link to "View the distribution of FIRST Teams around the world, per country".

## About FIRST

FIRST is the Forum of Incident Response and Security Teams. The idea of FIRST goes back until 1989, only one year after the CERT(r) Coordination Center was created after the infamous Internet worm. Back then incidents already were impacting not only one closed user group or organization, but any number of networks interconnected by the Internet.

It was clear from then on that information exchange and cooperation on issues of mutual interest like new vulnerabilities or wide ranging attacks - especially on core system like the DNS servers or the Internet as a critical infrastructure itself - were the key issues for security and incident response teams.

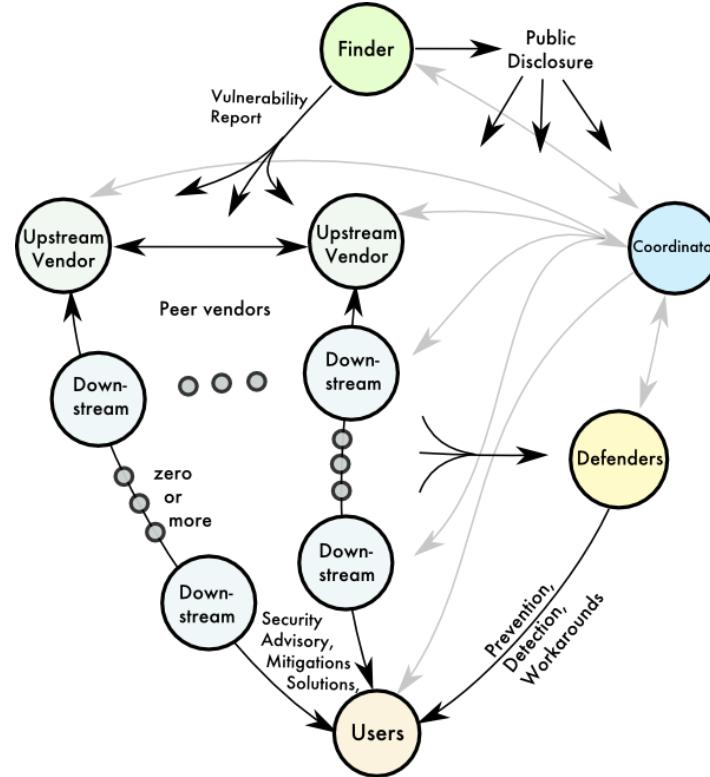
Since 1990, when FIRST was founded, its members have resolved an almost continuous stream of security-related attacks and incidents including handling thousands of security vulnerabilities affecting nearly all of the millions of computer systems and networks throughout the world connected by the ever growing Internet.

FIRST brings together a wide variety of security and incident response teams including especially product security teams from the government, commercial, and academic sectors.

View the distribution of FIRST Teams around the world, per country.

<https://first.org>

# Multi-Party Coordination



# Building an Incident Response Team

1

The first step to building a Computer Security Incident Response Team (CSIRT) is the decision and sponsorship by senior management of the creation of such team.

2

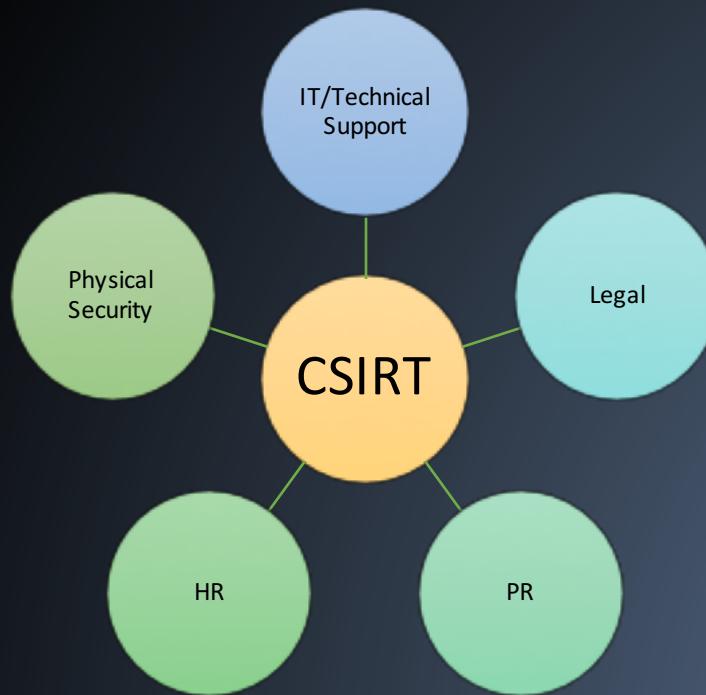
Then create the CSIRT charter including all the key elements that will drive the creation of such team.

# THE INCIDENT RESPONSE CHARTER SHOULD:

- Obtain senior leadership support
- Define the constituency
- Create a mission statement
- Outline the CSIRT service deliverables
- Proactive services
- Reactive services



# CSIRT Support Teams



# CSIRT Member Roles

- Incident Response Coordinators
- CSIRT Senior Analysts
- CSIRT Analysts
- Security Operations Center (SOC) Analyst
- IT Security Engineer / Analysts

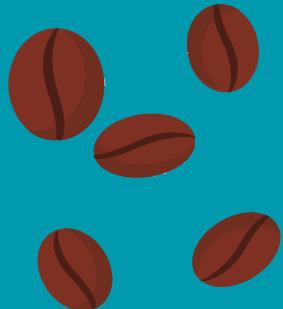


# External Collaboration

- A CSIRT may also need to interface with law enforcement and government agencies at times, especially if they are targeted as part of a larger attack perpetrated against a number of similar organizations.
- Having these relationships can help you with intelligence sharing and resources in the event of an incident.
- Examples:
  - High Technology Crime Investigation Association (HTCIA): <https://htcia.org>
  - Infragard: <https://www.infragard.org>
  - ISACs: <https://www.nationalisacs.org>
  - Local Law enforcement



# Break

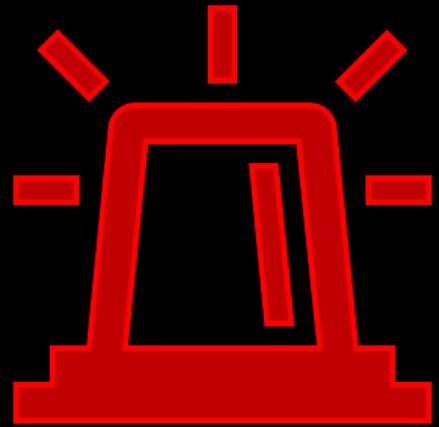


**Remember to check out the resources at:**

<https://h4cker.org>

<https://theartofhacking.org/training>

<https://theartofhacking.org/github>



# The Incident Response Plan

## **The policy elements described in NIST Special Publication 800-61 include:**

- Statement of management commitment
- Purpose and objectives of the incident response policy
- The scope of the incident response policy
- Definition of computer security incidents and related terms
- Organizational structure and definition of roles, responsibilities, and levels of authority
- Prioritization or severity ratings of incidents
- Performance measures
- Reporting and contact forms

## **NIST's incident response plan elements include the following:**

- Incident response plan's mission
- Strategies and goals of the incident response plan
- Senior management approval of the incident response plan
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization

NIST also defines standard operating procedures (SOPs) as:

“...a delineation of the specific technical processes, techniques, checklists, and forms used by the incident response team. SOPs should be reasonably comprehensive and detailed to ensure that the priorities of the organization are reflected in response operations.”

Not all incidents are equal in their severity and threat to the organization.

High-severity. Examples:

- Confirmed network intrusion
- Physical compromise of critical systems
- Compromise of critical accounts
- Targeted attacks and exfiltration of sensitive data

Moderate (medium) severity. Examples:

- Anticipated or ongoing DoS
- Confined malware infection
- Unusual system performance or behavior

Low severity incident. Examples:

- Lost or stolen mobile device containing encrypted confidential information.
- Policy or procedural violations

# Incident Tracking



Tracking incidents are a critical responsibility of the CSIRT.



All actions taken by the CSIRT and other personnel during an incident should be clearly documented during an incident.



Unique identifiers should be used.

# CISRT / Incident Tracking Tools



bestpractical/rt: Request Trackr

GitHub, Inc. [US] | https://github.com/bestpractical/rt

This repository Search Pull requests Issues Marketplace Explore

bestpractical / rt

Watch 72 Star 426 Fork 155

Code Pull requests 51 Projects 0 Insights

Request Tracker, an enterprise-grade issue tracking system <https://bestpractical.com/rt>

21,502 commits 132 branches 692 releases 68 contributors GPL-2.0

Branch: stable New pull request Create new file Upload files Find file Clone or download

cbrandtbuffalo Merge branch '4.4/disabled-user-in-single-custom-role' into 4.4-trunk Latest commit 4e6b89a 8 days ago

bin Update copyright for 2018 11 days ago

devel Merge branch '4.2-trunk' into 4.4-trunk 11 days ago

docs Merge branch '4.2-trunk' into 4.4-trunk 11 days ago

etc Update copyright for 2018 11 days ago

lib Show the user in single member custom roles even if the user is disabled 10 days ago

sbin Update copyright for 2018 11 days ago

share Indent fix 10 days ago

t Test AddWatcher with disabled user in single member custom role 9 days ago

.gitattributes Due to a git bug, be explicit about ignored directories 5 years ago

.gitignore ignore the generated rt-passwd from git a month ago

.perlcriticrc update perl critic policies 4 years ago

.perltidyrc Added a first draft perltidy for RT 8 years ago

COPYING README, COPYING and UPGRADE should not be executable 12 years ago

rt-4.4.2.tar.gz ... Show All X

Request Tracker

[GitHub, Inc. \[US\] | https://github.com/CrowdStrike/falcon-orchestrator](https://github.com/CrowdStrike/falcon-orchestrator)



CROWDSTRIKE  
**FALCON** ORCHESTRATOR

CrowdStrike Falcon Orchestrator is an extendable Windows-based application that provides workflow automation, case management and security response functionality. The tool leverages the highly extensible APIs contained within the CrowdStrike Falcon Connect program.

## Video Demonstration

---

Check out the following [video](#) on YouTube for a project overview and demonstration of Falcon Orchestrator.

## Support

---

As an open source project this software is not officially supported by CrowdStrike. As such we ask that you please refrain from sending inquiries to the CrowdStrike support team. The project maintainers will be working with active community contributors to address bugs and supply new features. If you have identified a bug please submit an issue through GitHub by following the contribution guidelines. You can also post questions or start conversations on the project through our [community forums](#) page.

You can also join the project chat room to discuss in greater detail, click [slack](#) 54 to sign up. Please note that the email you sign up with will be viewable by other users. If you wish to keep your company name anonymous you should use a personal email that holds no affiliation.

## Getting Started

opensourcesec/CIRTKit: Tools

GitHub, Inc. [US] | <https://github.com/opensourcesec/CIRTKit>

README.md

# CIRTKit

*One DFIR console to rule them all. Built on top of the [Viper Framework](#)*

---

[build](#) [unknown](#)

## Documentation

- Please see the [wiki](#) for more information about CIRTKit and documentation

## Roadmap

### Future integrations

- Bit9
- Palo Alto Networks
- EnCase/FTK

### Future modules

- Packet Analysis (possibly Dshell)
- Javascript Unpacking/Deobfuscation

Vulnerability Analysis Framework

CIRT Kit

A screenshot of a web browser displaying the Demisto Enterprise website at <https://www.demisto.com/>. The page features a dark background with a green digital wave pattern. At the top, there is a navigation bar with links for PRODUCT, WHY DEMISTO?, COMPANY, COMMUNITY, BLOG, PARTNERS, and RESOURCES. A red arrow points upwards from the bottom right towards the 'FREE COMMUNITY EDITION' button. The main title 'Demisto Enterprise' is prominently displayed in large white letters. Below it, the tagline 'The one and only product to unify' is shown. Three circular icons represent the product's features: INCIDENT MANAGEMENT, SECURITY ORCHESTRATION, and INTERACTIVE INVESTIGATION. A search icon is located at the bottom center.

DEMISTO

PRODUCT WHY DEMISTO? COMPANY COMMUNITY BLOG PARTNERS RESOURCES

FREE COMMUNITY EDITION

# Demisto Enterprise

The one and only product to unify

INCIDENT MANAGEMENT

SECURITY ORCHESTRATION

INTERACTIVE INVESTIGATION

Demistro

certsocietegenerale/FIR: Fast Incident Response · GitHub

GitHub, Inc. [US] | https://github.com/certsocietegenerale/FIR/

README.md

build passing

## What is FIR? Who is it for?

FIR (Fast Incident Response) is an cybersecurity incident management platform designed with agility and speed in mind. It allows for easy creation, tracking, and reporting of cybersecurity incidents.

FIR is for anyone needing to track cybersecurity incidents (CSIRTs, CERTs, SOCs, etc.). It's was tailored to suit our needs and our team's habits, but we put a great deal of effort into making it as generic as possible before releasing it so that other teams around the world may also use it and customize it as they see fit.

STARRED INCIDENTS

Date	Category	Subject	Business Lines	Severity	Status	Detection	Leader	Last Action	Plan	Lvl	IH	Edit
2015-03-10	★ Phishing	http://phishingsite.com/url/	Sub BL 1	2	Open	CERT	CERT	Abuse 16 hours ago	B	C1	dev	edit

Open Blocked Old Tasks

Date	Category	Subject	Business Lines	Severity	Status	Detection	Leader	Last Action	Plan	Lvl	IH	Edit
2015-03-10	★ Phishing	http://phishingsite.com/url/	Sub BL 1	2	Open	CERT	CERT	Abuse 16 hours ago	B	C1	dev	edit
2015-01-15	★ Phishing	test	Demo BusinessLine 1	1	Open	CERT	None	Opened 2 months ago	None	C1	dev	edit
2015-01-05	★ Phishing	test	Demo BusinessLine 1, Demo BusinessLine 2	2	Open	Pôle	None	Alerting 2 months ago	None	C1	dev	edit
2015-01-05	★ Phishing	test	Demo BusinessLine 1, Demo BusinessLine 2	2	Open	Pôle	None	Opened 2 months ago	None	C1	dev	edit
2014-12-17	★ IS integrity	Alerte Jokeware	Demo BusinessLine 1	1	Open	SOC	None	Opened 3 months ago	None	C1	dev	edit
2014-12-17	★ Phishing	phishing	Demo BusinessLine 1, Demo BusinessLine 2	2	Open	CERT	CERT	Info 3 months ago	B	C1	dev	edit

(page 1 of 1)

FIR | New event | Dashboard | Incidents | Events | Stats | search... | Currently logged in as dev | Logout | Admin |

Instant Leader: None | Plan: None | Severity: 1 | Category: Phishing | Status: Closed | Detection: CERT | BL: Demo BusinessLine 1

### Incident / Phishing / test

Opened on Jan. 15, 2015, 8:47 p.m. by dev

DESCRIPTION	CORRELATED ARTIFACTS
phishing copying our brand website on http://evilwebsite.com/leadurl	Type: Values Hostnames: evilwebsite.com (1) X

Fast Incident Response (FIR)

sandialabs/scot: Sandia Cyber

GitHub, Inc. [US] | https://github.com/sandialabs/scot

This repository Search Pull requests Issues Marketplace Explore

Watch 38 Star 164 Fork 37

sandialabs / scot

Code Issues 2 Pull requests 0 Projects 0 Wiki Insights

Sandia Cyber Omni Tracker (SCOT) <http://getscot.sandia.gov>

perl javascript cyber-security incident-response

7,787 commits 3 branches 6 releases 10 contributors

Branch: master New pull request Create new file Upload files Find file Clone or download

brymon68 Merge branch 'master' of baltig.sandia.gov:scot/SCOT Latest commit 28ee11c 23 days ago

File	Description	Time Ago
bin	testing programs for queue	a month ago
demo	adding env to demo	a month ago
docker-configs	fixes to open source mongo and commented out ldap stuffs	a month ago
docker-scripts	update to restore script for docker	2 months ago
docs	Preliminary work for beamup	2 months ago
etc	so close, so close	a year ago
install	updating default config files	a month ago
lib	undiscovered regex bug in sourcefire parser	23 days ago
pkgs	Initial SCOT release	4 years ago
pubdev	Merge branch 'master' of baltig.sandia.gov:scot/SCOT	24 days ago
public	added remove event emitter functionality when changing between ids	24 days ago
script	Initial SCOT release	4 years ago

Sandia Cyber Omni Tracker (SCOT)

defpoint/threat\_note: DPS' Light... | GitHub, Inc. [US] | https://github.com/defpoint/threat\_note

Omar

This repository Search Pull requests Issues Marketplace Explore

Watch 52 Star 286 Fork 72

Code Issues 43 Pull requests 1 Projects 0 Wiki Insights

### DPS' Lightweight Investigation Notebook

396 commits 2 branches 0 releases 11 contributors Apache-2.0

Branch: master New pull request Create new file Upload files Find file Clone or download

null brianwarehime Merge pull request #163 from k3vb0t/master ... Latest commit 7c56e5a on Aug 15, 2016

File	Description	Time Ago
docker	Resolved dependency issues.	2 years ago
threat_note	Fixed error with cuckoo database, added some(albeit way to many) exce...	2 years ago
.editorconfig	added html specific editorconfig	2 years ago
.gitignore	expanded venv ignore	2 years ago
.pre-commit-config.yaml	added simple precommit hook	2 years ago
CONTRIBUTING.md	added development requirements and how to set it up	2 years ago
LICENSE	Initial commit	3 years ago
Procfile	Change server back to threat_note	2 years ago
README.md	Minor update to include web address.	2 years ago
requirements-dev.txt	Updated to reflect changes to ODNS API	2 years ago
requirements.txt	Updated to reflect changes to ODNS API	2 years ago

threat\_note

Cyphon

Secure | https://www.cyphon.io

Omar

[download](#) [faqs](#) [updates](#) [technology](#) [home](#)

An Open Source Incident Management and Response Platform

Cyphon eliminates the headaches of incident management by streamlining a multitude of related tasks through a single platform. It receives, processes and triages events to provide an all-encompassing solution for your analytic workflow — aggregating data, bundling and prioritizing alerts, and empowering analysts to investigate and document incidents.

INCIDENT MANAGEMENT SOLUTION

Cyphon

Security Operations | Enterprise X

Omar

Secure | https://www.servicenow.com/products/security-operations.html

service<sup>now</sup>

PRODUCTS SOLUTIONS SERVICES & SUPPORT PARTNERS EVENTS ABOUT US

SEARCH GLOBE MORE



DEMO NOW

Call icon

SERVICENOW SECURITY OPERATIONS

## Identify, Prioritize, and Respond to Threats Faster

ServiceNow® Security Operations is an Enterprise Security Response engine offering security incident response, vulnerability response, configuration compliance, and threat intelligence. It's built on the intelligent workflows, automation, orchestration, and deep connection with IT of the ServiceNow platform.

ServiceNOW (commercial)

# Incident Response Playbooks

Playbooks help with:

- Incident detection
- Response actions
- Communication

## Why Create a Playbook?

The purpose of a security playbook is to provide all stakeholders with a clear understanding of their responsibilities and procedures before, during, and after a security incident.

Playbooks can't respond  
to incidents on their own



\* ownership

\* follow-up

\* comms



# Scheduling

- real-time necessary ?
- enough analysts to keep up ?
- when to escalate ?

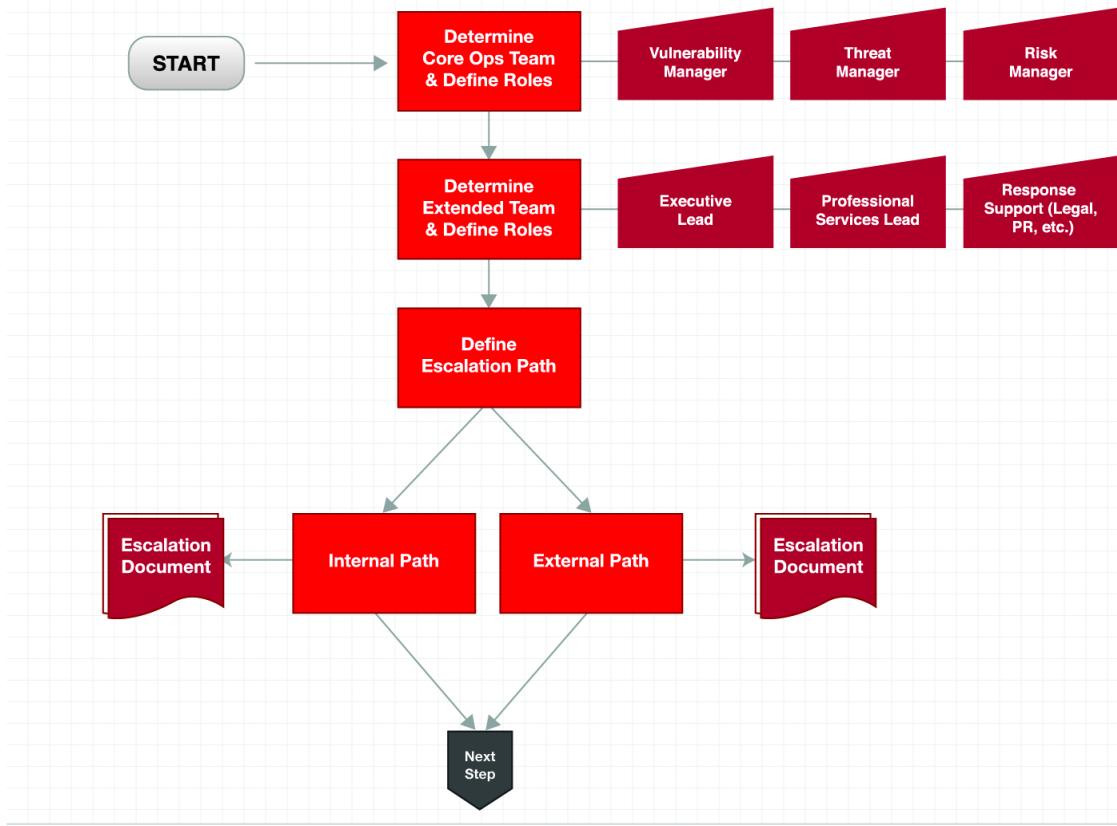
Metrics?



- What to do to avoid duplicate events, tickets, and incidents ?
- What mitigating capabilities and supporting policies exist ?

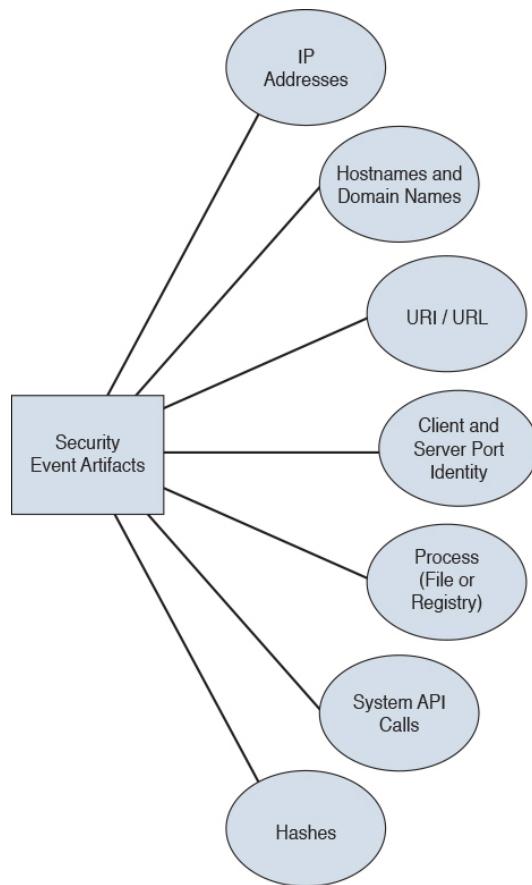
# REACT

- Review policies and procedures
- Evaluate the situation
- Avoid panic
- Collect information
- Take appropriate action



DEMO

<https://www.incidentresponse.com/playbooks>



# ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	ApnInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	ApnInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Datafuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Remain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-Stage Channels
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	LSASS Driver	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	SSH Hijacking	Screen Capture		Multiband Communication
			Image File							

ATT&amp;CK

Cyber Threat Intelligence Tech x

Secure | <https://oasis-open.github.io/cti-documentation/>

Omar

Home STIX TAXII Contribute FAQ Resources

Looking for... STIX 1.x? TAXII 1.x?

## Sharing threat intelligence just got a lot easier!

### STIX™

A structured language for cyber threat intelligence

Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI). STIX enables organizations to share CTI with one another in a consistent and machine readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively. STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.

STIX Relationship Example

[Learn More](#)

### TAXII™

A transport mechanism for sharing cyber threat intelligence

Trusted Automated Exchange of Intelligence Information (TAXII™) is an application layer protocol for the communication of cyber threat information in a simple and scalable manner. TAXII is a protocol used to exchange cyber threat intelligence (CTI) over HTTPS. TAXII enables organizations to share CTI by defining an API that aligns with common sharing models. TAXII is specifically designed to support the exchange of CTI represented in STIX.

TAXII Collections

[Learn More](#)

<https://oasis-open.github.io/cti-documentation/>

# Break

**Remember to check out the resources at:**

<https://h4cker.org>

<https://h4cker.org/training>

<https://h4cker.org/github>





Digital Forensics Fundamentals



Cybersecurity forensics (or digital forensics) has been of growing interest among many organizations and individuals due to the large number of breaches during the last few years.

# Three broad categories of cybersecurity investigations:

- Public investigations: These investigations are resolved in the court of law.
- Private investigations: These are corporate investigations.
- Individual investigations: These investigations often take the form of e-discovery.



[https://www.youtube.com/watch?v=9Mp261PDi\\_E](https://www.youtube.com/watch?v=9Mp261PDi_E)

# Collecting Evidence from Endpoints and Servers

- Cybersecurity forensic evidence can take many forms, depending on the conditions of each case and the devices from which the evidence was collected.
- To prevent or minimize contamination of the suspect's source device, you can use different tools, such as a piece of hardware called a write blocker, on the specific device so you can copy all the data (or an image of the system).

# There are three general types of evidence



- Best evidence
- Corroborating evidence
- Indirect or circumstantial evidence

# Evidence Preservation

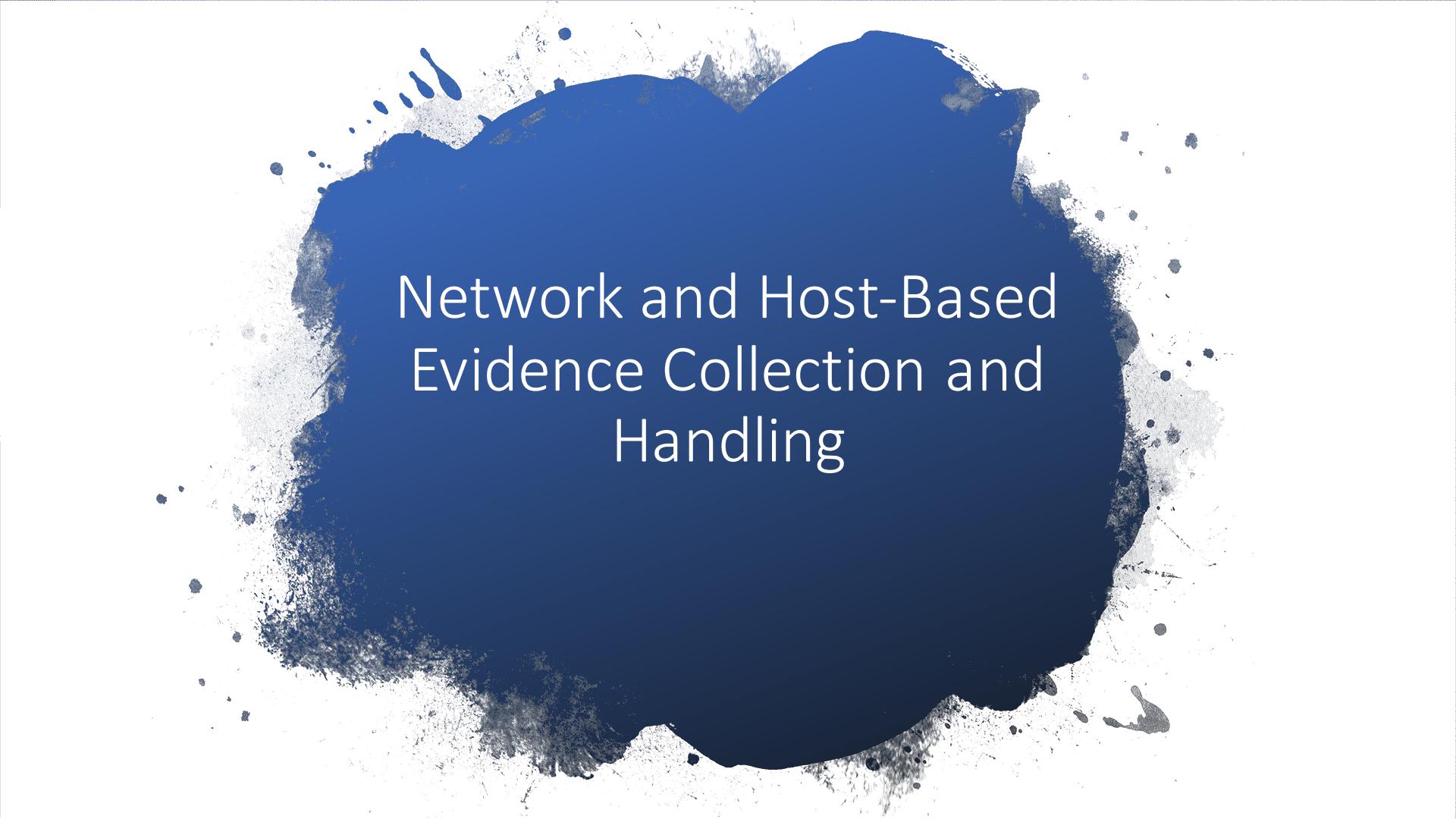
- Use write-protected storage devices.
- The storage device you are investigating should immediately be write-protected before it is imaged and should be labeled to include the following:
  - Investigator's name
  - The date when the image was created
  - Case name and number (if applicable)

<http://h4cker.org/dfir/lrt4.html>

# Chain of Custody

- Chain of custody is the way you document and preserve evidence from the time that you started the cyber forensics investigation to the time the evidence is presented in court.
- It is extremely important to be able to show clear documentation of the following:
  - How the evidence was collected
  - When it was collected
  - How it was transported
  - How it was tracked
  - How it was stored
  - Who had access to the evidence and how it was accessed

<http://h4cker.org/dfir/int4.html>



# Network and Host-Based Evidence Collection and Handling

# Imaging Process in Digital / Cyber Forensics

- The imaging process is intended to copy all blocks of data from the computing device to the forensics professional evidentiary system.
- This is sometimes referred to as a “physical copy” of all data, as distinct from a logical copy, which only copies what a user would normally see.
- Logical copies do not capture all the data, and the process will alter some file metadata to the extent that its forensic value is greatly diminished, resulting in a possible legal challenge by the opposing legal team.
- Therefore, a full bit-for-bit copy is the preferred forensic process.
- The file created on the target device is called a forensic image file.

# The Most Common File Types for Forensic Images

- .AFF
- .ASB
- .E01
- .DD or raw image files
- Virtual image formats such as .VMDK and .VDI

# SANS Forensics Resource



Interested in learning  
more about security?

## SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

### An Overview of Disk Imaging Tool in Computer Forensics

The objective of this paper is to educate users on disk imaging tool ; issues that arise in using disk imaging, recommended solutions to these issues and examples of disk imaging tool. Eventually the goal is to guide users to choose the right disk imaging tool in computer forensics.

<https://www.sans.org/reading-room/whitepapers/incident/overview-disk-imaging-tool-computer-forensics-643>

# Collecting Evidence from Mobile Devices

- Mobile devices such as cell phones, wearables, and tablets are not imaged in the same way as desktops.
- Also, today's Internet of Things (IoT) world is very different from just a few years ago.
- The hardware and interfaces of these devices, from a forensic perspective, are very different.
- In some cases, not only does evidence need to be collected from mobile devices, but also from mobile device management (MDM) applications and solutions.

# Collecting Evidence from Network Infrastructure Devices

- Syslog
- DHCP events
- NetFlow
- Authentication, authorization, and accounting (AAA) logs
- VPN logs
- Firewall logs

<http://h4cker.org/dfir/irt4.html>

# Digital Forensic Tools



The Sleuth Kit (TSK) & Autopsy X

Secure | https://www.sleuthkit.org/index.php

Home Autopsy The Sleuth Kit Other Projects Support About

## Open Source Digital Forensics



**Autopsy®** is an easy to use, GUI-based program that allows you to efficiently analyze hard drives and smart phones. It has a plug-in architecture that allows you to find add-on modules or develop custom modules in Java or Python.

**The Sleuth Kit®** is a collection of command line tools and a C library that allows you to analyze disk images and recover files from them. It is used behind the scenes in Autopsy and many other open source and commercial forensics tools.

These tools are used by thousands of users around the world and have community-based e-mail lists and forums. Commercial training, support, and custom development is available from [Basis Technology](#).

[Follow @sleuthkit](#)

### Latest News

14 MAR Linux Autopsy 4.6.0 (beta 1) released First incremental release. 90% complete.

22 FEB Autopsy 4.6.0 released Communications UI, Central Hash DB, USB Triage Drive and more.

21 FEB The Sleuth Kit 4.6.0 released Communications-related DB tables and Java classes. C fixes.

15 OCT The Sleuth Kit 4.5.0 released LZVN HFS+ compression, E01 Sector sizes, and more.

13 OCT Autopsy 4.5.0 released New Correlation Engine, memory improvements and more.

8 AUG Autopsy 4.4.1 released New beta correlation engine and various fixes.

EnCase Endpoint Security - En X

Secure | https://www.guidancesoftware.com/encke-endpoint-security

GUIDANCE SOFTWARE is now opentext™

Got Breached? Q

NEED HELP?

# EnCase® Endpoint Security

Earlier Detection, Faster Decisions and Unprecedented Threat Response.

Advanced Detection      Automated Alert Response      New User Interface      New Simplified Workflows

**JUST RELEASED:**

## EnCase Endpoint Security 6.04

EnCase Endpoint Security 6.04 delivers feature enhancements focused on security-first workflows including a fully bi-directional Splunk integration and a new Snapshot Comparison feature. These capabilities provide incident responders with greater automation and contextualization of security alerts, resulting in faster decision-making and improved security efficacy.

[What's New »](#)

[Request Demo »](#)

THE ONLY 360° VISIBILITY INTO THE ENDPOINT

EnCase

Forensic Toolkit Omar

Secure | <https://accessdata.com/products-services/forensic-toolkit-ftk>

Live Support Chat | Sales +1 800 574 5199

CONTACT US SUPPORT

 ACCESSDATA

Products & Services Industries Customer Stories Resources Training Partners About



**FORENSIC TOOLKIT (FTK)**  
Digital Investigations

[Video](#) | [Features](#) | [Capabilities](#) | [Case Studies](#) | [Infographic](#) | [Testimony](#) | [Resources](#) | [Related Products & Services](#)

## Why You Want It

Zero in on relevant evidence quickly, conduct faster searches and dramatically increase analysis speed with FTK®, the purpose-built solution that interoperates with mobile device and e-discovery technology. Powerful and proven, FTK processes and indexes data upfront, eliminating wasted time waiting for searches to execute. No matter how many different data sources you're dealing with or the amount of data you have to cull through, FTK gets you there quicker and better than anything else.

**UNMATCHED SPEED AND STABILITY**  
FTK uses distributed processing and is the only forensics solution to fully leverage multi-

**FASTER SEARCHING**  
Since indexing is done up front, filtering and searching are completed more efficiently than with

**DATABASE DRIVEN**  
FTK is truly database driven, using one shared case database. All data is stored securely and centrally,

[Leave a message](#) TOP

Access Data Forensics Toolkit

Security-Onion-Solutions/security-onion

GitHub, Inc. [US] | https://github.com/Security-Onion-Solutions/security-onion

This repository Search Pull requests Issues Marketplace Explore

Watch 263 Star 1,413 Fork 214

Code Issues 90 Pull requests 0 Projects 2 Wiki Insights

Linux distro for IDS, NSM, and Log Management <https://securityonion.net>

intrusion-detection network-security-monitoring log-management ids nsm hunting dfir

2,309 commits 3 branches 21 releases 2 contributors

Branch: master New pull request Create new file Upload files Find file Clone or download

dougburks promote 14.04.5.13 to stable Latest commit 0300d9b 5 days ago

.github	add ISSUE_TEMPLATE	a year ago
old	promote 14.04.5.13 to stable	5 days ago
sigs	update sigs and testing instructions for 14.04.5.13	11 days ago
KEYS	Create KEYS	2 years ago
README.md	promote 14.04.5.11 to stable	27 days ago
Verify_ISO.md	promote 14.04.5.13 to stable	5 days ago
checksums.txt	update sigs and testing instructions for 14.04.5.13	11 days ago

README.md

## Security Onion

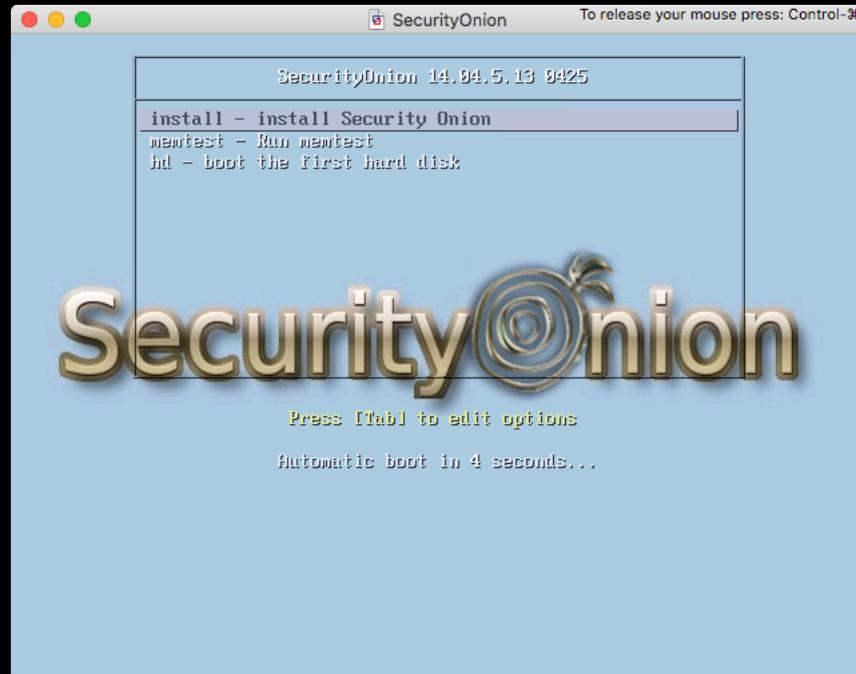
Security Onion is a free and open source Linux distribution for intrusion detection, enterprise security monitoring, and log management. It includes Elasticsearch, Logstash, Kibana, Snort, Suricata, Bro, OSSEC, Sguil, Squert, NetworkMiner, and many other security tools. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!

For more information about Security Onion, please see our [main website](#), [blog](#), and [wiki](#).

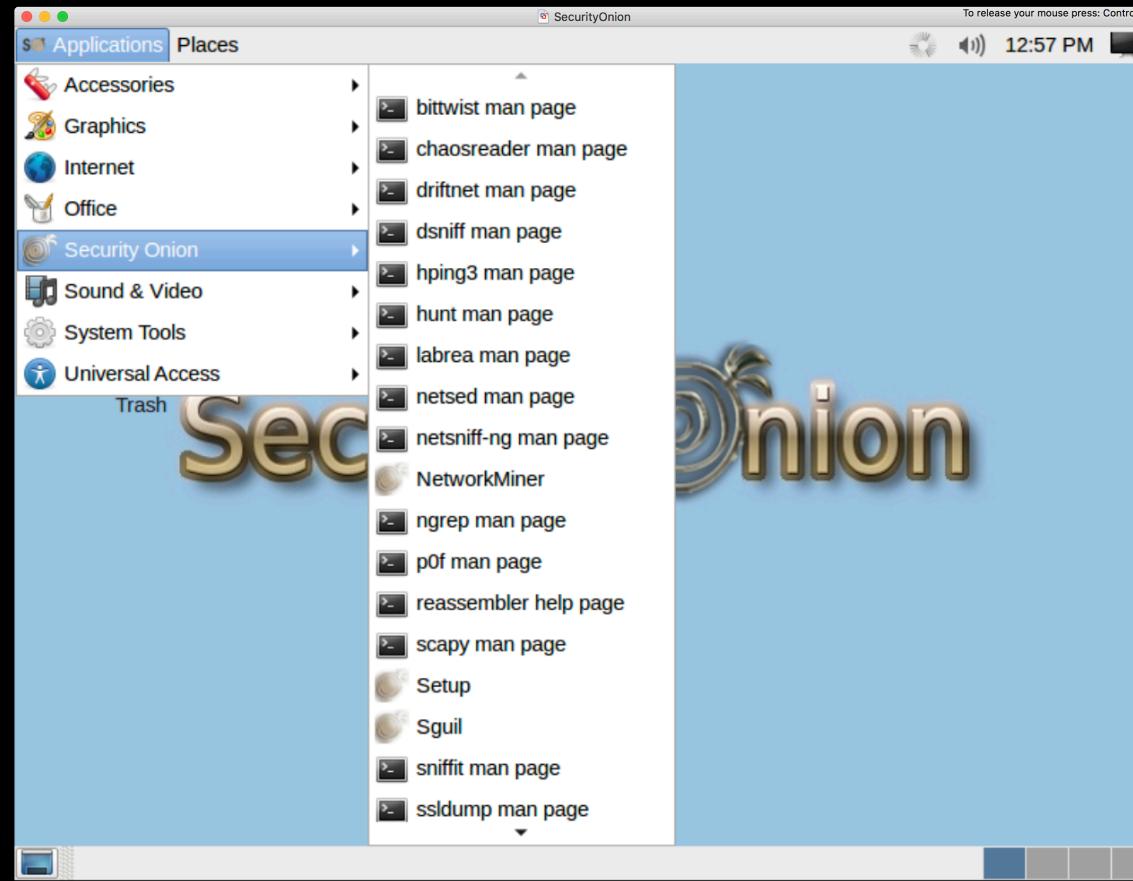
### This Repo

This repo contains the [ISO image](#), [Wiki](#), and [Roadmap](#) for Security Onion.

Security Onion



Security Onion



Security Onion

Linux Forensics Tools Repository | CERT Division

CMU SEI CERT Division Digital Library Blogs

CERT Software Engineering Institute Carnegie Mellon University

## Linux Forensics Tools Repository - LiFTeR

### Welcome

Welcome to the CERT Linux Forensics Tools Repository (LiFTeR), a repository of packages for Linux distributions. Currently, Fedora and CentOS/RHEL are provided in the repository. See here for the Fedora version support table and here for the CentOS/RHEL version support table. If you are interested in porting the repository to other versions of Linux, please see the Contribute section.

The CERT Linux Forensics Tools Repository provides many useful packages for cyber forensics acquisition and analysis practitioners. If you have suggestions for tools to add to the repository, please see the Contribute section.

The CERT Linux Forensics Tools Repository is not a standalone repository, but rather an extension of the supported systems. Tools can be installed as needed or all at once using the CERT-Forensics-Tools meta package.

Also described here is ADIA, the VMware-based Appliance for Digital Investigation and Analysis. ADIA is a Fedora-based VMware guest intended to be installed under VMware Workstation, Player, or Fusion. It is not a Live CD. See the ADIA section for more details.

### NOTICE - IMPORTANT Items Shown In Red

Important items are now shown in red. Pay attention to them because they are important.

### Contents

- NOTICE - New RPM Signing Key - February, 2016
- End Of Life Announcement
- Repository RSYNC Server
- Announcements
  - All
  - Recent

### Announcements

- By Package
- By Date
- All Announcements

**April 27, 2018**

[Pfring](#)  
PFRing, version 7.0.0 release 1887, was installed in the CentOS/RHEL 6 and 7 repositories for the x86\_64 architecture.

[Pfring-dkms](#)  
PFRing-dkms, version 7.0.0 release 1887, was installed in the CentOS/RHEL 6 and 7 repositories for the x86\_64 architecture.

[APFS-Fuse](#)  
APFS-Fuse, version 20180424 release 1, was installed in the Fedora 22, 23, 24, 25, 26, and 27 repositories for all supported architectures, and the CentOS/RHEL 7 repositories for the x86\_64 architecture.

[Aimage](#)  
Aimage, version 3.2.5 release 3, was installed in the CentOS/RHEL 6 and 7 repositories for all supported architectures.

[CERT-Forensics-Tools](#)  
CERT-Forensics-Tools, version 1.0 release 75, was installed in the Fedora 22, 23, 24, 25, 26, and 27 repositories for all supported architectures, and the CentOS/RHEL 6 and 7 repositories for all supported architectures.

[examiner-tooldocumentation](#)  
Examiner-Tooldocumentation, version 1.18 release 6, was installed in the CentOS/RHEL 7 repository for the x86\_64 architecture.

[LIME](#)  
Lime-kernel-modules-fc27-{i686,x86\_64}, version 1.1.r17 release 22, were installed in the Fedora 22, 23, 24, 25, 26, and 27 repositories for all

ADIA - The Appliance for Digital Investigation and Analysis

Secure | https://forensics.cert.org/appliance/README.html



## ADIA - The Appliance for Digital Investigation and Analysis

### CentOS 7 Version

This README describes the virtual machine image for ADIA, the Appliance for Digital Investigation and Analysis. These virtual machines are based on CentOS 7.

This version of ADIA supports both VMware and Virtual Box. This version support the x86\_64 (64 bit) host computer system architecture.

You should routinely update ADIA to keep it current with package released by Red Hat and packages released by CERT.

#### Installation - VMware

ADIA has been tested and works on VMware Workstation 14 under Windows 10 Education. We expect that it will work in other configurations but they remain untested. When the virtual machine was packaged for distribution, it was converted to work with VMware Workstation 5 and later.

To install ADIA under VMware, do the following:

1. Download the VMware-based [OVA](#).
2. Optionally check the [PGP/GPG Signature](#).
3. Start VMware.
4. Select [File->Import....](#).
5. Navigate to the downloaded OVA and select it.
6. Import the virtual machine.
7. If you get an [Import Failed](#) error message, select [Retry](#) to continue.
8. Select the [Continue](#) button to continue.
9. When the import finishes, select the [Finish](#) button to continue.
10. Optionally update the hardware version of the newly created virtual machine.
11. Start the virtual machine.
12. The virtual machine will boot and automatically login as examiner (with password forensics).
13. This version of ADIA uses the the [MATE Desktop Environment](#).

Installing ADIA under VMware requires about 8Gb of disk space.

#### Installation - Virtual Box

ADIA has been tested and works on Virtual Box 5.2.2 under Windows 10 Education. We expect that it will work in other configurations but they remain untested.

About | DEFT Linux - Compute X Omar

www.deftlinux.net/about/

# deft

Home About » Download Package list DEFT Manual Screenshot Contacts

## About

DEFT (acronym for Digital Evidence & Forensics Toolkit) is a distribution made for Computer Forensics, with the purpose of running live on systems without tampering or corrupting devices (hard disks, pendrives, etc...) connected to the PC where the boot process takes place.

The DEFT system is based on GNU Linux, it can run live (via DVDROM or USB pendrive), installed or run as a Virtual Appliance on VMware or Virtualbox. DEFT employs LXDE as desktop environment and WINE for executing Windows tools under Linux. It features a comfortable mount manager for device management.

DEFT is paired with DART (acronym for Digital Advanced Response Toolkit), a Forensics System which can be run on Windows and contains the best tools for Forensics and Incident Response. DART features a GUI with logging and integrity check for the instruments here contained.

Besides all this, the DEFT staff is devoted to implementing and developing applications which are released to Law Enforcement Officers, such as Autopsy 3 for Linux.

DEFT is currently employed in several places and by several people such as:

- Military
- Government Officers
- Law Enforcement
- Investigators
- Expert Witnesses
- IT Auditors
- Universities
- Individuals

Languages

English

Donate

1DEFTAYfqK76woMv9U9o2rD4n3vWVCJLm

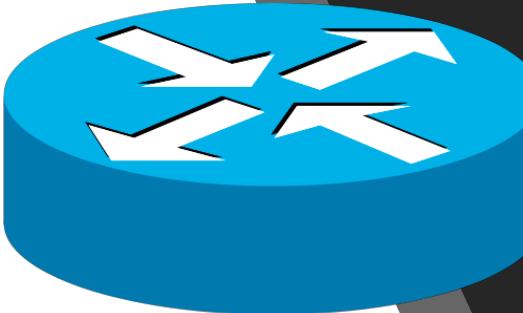
Search

Search

deft

# Infrastructure Devices

- A lot of people have an understanding and tools to perform forensics on Endpoints and Servers (Linux, OS X, Windows, etc).
- However, there is a shortage of knowledge on how to perform forensics and integrity verification in infrastructure devices (routers, switches, firewalls, etc.)



# Infrastructure Device Integrity Assurance and Verification

- Cisco IOS Device Integrity Assurance:
  - <https://www.cisco.com/c/en/us/about/security-center/integrity-assurance.html>
- Cisco IOS-XE Device Integrity Assurance:
  - <https://www.cisco.com/c/en/us/about/security-center/ios-xe-integrity-assurance.html>
- Cisco ASA Device Integrity Assurance:
  - <https://www.cisco.com/c/en/us/about/security-center/intelligence/asa-integrity-assurance.html>

The screenshot shows a GitHub repository page for 'The-Art-of-Hacking / art-of-hacking'. The repository has 20 stars, 65 forks, and 22 open issues. A pull request titled 'adding DFIR references' has been merged. The README.md file contains a section titled 'Digital Forensics and Incident Response (DFIR) Resources' which lists several tools and resources for incident response.

## Digital Forensics and Incident Response (DFIR) Resources

### Incident Response

- [Cyphon](#) - Cyphon eliminates the headaches of incident management by streamlining a multitude of related tasks through a single platform. It receives, processes and triages events to provide an all-encompassing solution for your analytic workflow — aggregating data, bundling and prioritizing alerts, and empowering analysts to investigate and document incidents.
- [Demisto](#) - Demisto community edition(free) offers full Incident lifecycle management, Incident Closure Reports, team assignments and collaboration, and many integrations to enhance automations (like Active Directory, PagerDuty, Jira and much more..)
- [FIR](#) - Fast Incident Response (FIR) is an cybersecurity incident management platform designed with agility and speed in mind. It allows for easy creation, tracking, and reporting of cybersecurity incidents and is useful for CSIRTs, CERTs and SOCs alike
- [RTIR](#) - Request Tracker for Incident Response (RTIR) is the premier open source incident handling system targeted for computer security teams. We worked with over a dozen CERT and CSIRT teams around the world to help you handle the ever-increasing volume of incident reports. RTIR builds on all the features of Request Tracker
- [SCOT](#) - Sandia Cyber Omni Tracker (SCOT) is an Incident Response collaboration and knowledge capture tool focused on flexibility and ease of use. Our goal is to add value to the incident response process without burdening the user
- [threat\\_note](#) - A lightweight investigation notebook that allows security researchers the ability to register and retrieve indicators related to their research

### Playbooks

<https://github.com/The-Art-of-Hacking/art-of-hacking/tree/master/dfir>

QUESTIONS?

THANK YOU!