



# Cybersecurity: Where to Start

## Who Am I?

John Helme

Senior Security Analyst

Utility Services

[John.Helme@utilitysvcs.com](mailto:John.Helme@utilitysvcs.com)



Started working on computers in 1977 with a Radio Shack TRS-80.

Have certifications to work on systems that have not been operational this century.

Started working in the electric utility industry in 2010.

Told coworkers to use “age appropriate language” when texting me. I don’t know what all of the TLAs mean.

## What the program said I am talking about:

Cyber threats are real risks to small utilities and municipalities. Staying up to date on cybersecurity trends is essential and **can have components which are inexpensive, as long as you donate your time\***. In fact, many free resources are available to assist. Attendees will learn best practices for developing awareness and incorporating simple, low-cost measures that can go a long way and make a real impact. When it comes to cybersecurity, doing nothing isn't an option.

**\*Edits that were not included in the program.**

# Is it Cybersecurity, Cyber Security or Cyber-Security?

“American style tends to favor **cybersecurity** as one word while British style often uses **Cybersecurity** as two words.

... **Cybersecurity** and **Cybersecurity** have the same meaning. (And while you might catch “**cyber-security**” here and there, it means the same and is not a widely-used or preferred derivative).

<https://threatwarrior.com/blog/cyber-security-one-word-or-two/>



# DHS and Homeland Security

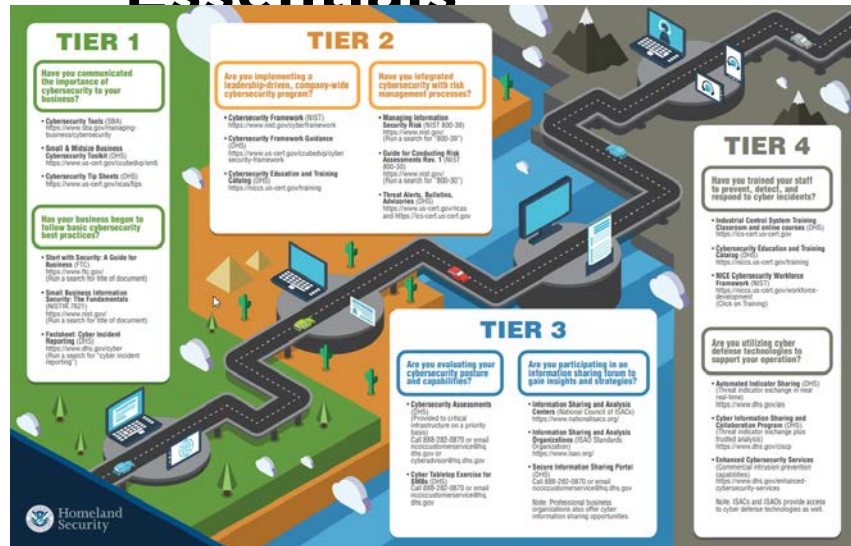
## CISA Resources for Small and Midsize Businesses

<https://www.us-cert.gov/resources/smb>

## Cyber Security Road Map Essentials

## Cyber Resilience

## Cyber



**Homeland Security**

### CYBER RESILIENCE REVIEW

The Department of Homeland Security (DHS) offers the Cyber Resilience Review (CRR) as a voluntary, no-cost tool for critical infrastructure organizations and state, local, tribal, and territorial governments. Provided by regionally located Cybersecurity Advisors, the CRR offers insights into an organization's operational resilience and cybersecurity capabilities.

**FORMAT AND GOAL**  
DHS offers two options for the CRR: a downloadable self-assessment and a facilitated six-hour session with trained DHS representatives at your location. Through the CRR, your organization will develop an understanding of its operational resilience and ability to manage cyber risk during normal operations and times of operational stress and crisis.

**APPROACH**  
The CRR is derived from the Cyber Resilience Management Model (CRRMM), a process improvement model developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience. The CRR is based on the premise that an organization deploys its assets (people, information, technology, and facilities) to support specific critical services or products. Based on this principle, the CRR evaluates the maturity of your organization's operations and capabilities in performing planning, managing, training and defining cybersecurity capabilities across 10 domains:

1. Asset Management
2. Configuration and Change Management
3. Vulnerability Management
4. Incident Management
5. Service Continuity Management
6. Risk Management
7. External Dependency Management
8. Training and Awareness
9. Information Management
10. Situational Awareness

**CISA**

### CYBER ESSENTIALS

Your success depends on Cyber Readiness. Both depend on YOU.

## THE LEADER'S GUIDE

Reducing your organization's cyber risks requires a holistic approach - similar to the approach you would take to address other operational risks. As with other risks, cyber risks can threaten:

- YOUR ABILITY TO OPERATE / ACCESS INFO
- YOUR REPUTATION / CUSTOMER TRUST
- YOUR BOTTOM LINE
- YOUR ORGANIZATION'S SURVIVAL

Managing cyber risks requires building a culture of cyber readiness.

### Essential Elements of a Culture of Cyber Readiness:

Yourself	Your Staff	Your Systems
<b>The Leader</b> Drive cybersecurity strategy, investment and culture. Your awareness of the basics drives cybersecurity to be a major part of your operational resilience strategy, and that strategy requires an investment of time and money. Your investment drives actions and activities that build and sustain a culture of cybersecurity.	<b>The Staff</b> Develop security awareness and vigilance. Your staff will often be your first line of defense, one that must have - and continuously grow - the skills to practice and maintain readiness against cybersecurity risks.	<b>What Makes You Operational</b> Protect critical assets and applications. Information is the lifeblood of any business; it is often the most valuable of a business' intangible assets. Know where this information resides, know what applications and networks store and process that information, and build security into and around these.

Your Surroundings	Your Data	Your Actions Under Stress
<b>The Digital Workplace</b> Ensure only those who belong to your digital workplace have access. The authority and access you grant employees, managers, and customers into your digital environment needs limits, just as those set in the physical work environment do. Setting approved access privileges requires knowing who operates on your systems and with what level of authorization and accountability.	<b>What the Business is Built On</b> Make backups and avoid the loss of information critical to operations. Even the best security measures can be circumvented with a patient, sophisticated adversary. Learn to protect your information where it is stored, processed, and transmitted. Have a contingency plan, which generally starts with being able to recover systems, networks, and data from known, accurate backups.	<b>Limit damage and quicken restoration of normal operations</b> The strategy for responding to and recovering from compromise: plan, prepare for, and conduct drills for cyberattacks as you would a fire. Make your reaction to cyberattacks and system failures an extension of your other business contingency plans. This requires having established procedures, trained staff, and knowing how - and to whom - to communicate during a crisis.

VOL. 1, FALL 2019  
CISA.gov/Cyber-Essentials  
For tech specs on building a Culture of Cyber Readiness, flip page ▶



# **Do you really have a Cybersecurity Program?**

- Does the program have buy-in from all individuals in the organization?
- Are the applicable portions of the program available to individuals that use the systems?
- Is the program based on risk management and not just implementation of technology?
- Does your program include both the control systems and the administrative systems?
- Does your program require the separation of the control and administrative system?

# Tools for developing a Cybersecurity Program

## Frameworks or Models

- PCI DSS - Payment Card Industry Data Security Standard
  - [https://www.pcisecuritystandards.org/pci\\_security/](https://www.pcisecuritystandards.org/pci_security/)
- ISO 27001/27002 - Information technology – Security techniques
  - <https://www.iso27001security.com/html/27001.html>
- CIS Critical Security Controls
  - <https://www.sans.org/critical-security-controls/>
- NIST Framework for Improving Critical Infrastructure Security
  - <https://www.nist.gov/cyberframework>
- NERC CIP Standards
  - <https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>

# Is your Cybersecurity Program based on Risk?

Is the program based on available technology or budget?

Is the program seen as a one-time project?

Is the program still “owned” by any single person or any single group?

Does the plan cover all of the cyber systems?

Has risk been considered when developing the plan?

Threats

Vulnerabilities

Consequences

Probability

# Components of a Cybersecurity

## • Training and Awareness

- Are you utilizing effective training and awareness materials?
- Are they received by all people in all departments?

## • Tools

- October – Cyber Security Awareness Month
- Schweitzer Engineering Laboratories
  - <https://selinc.com/solutions/sfci/cybersecurity-posters/>

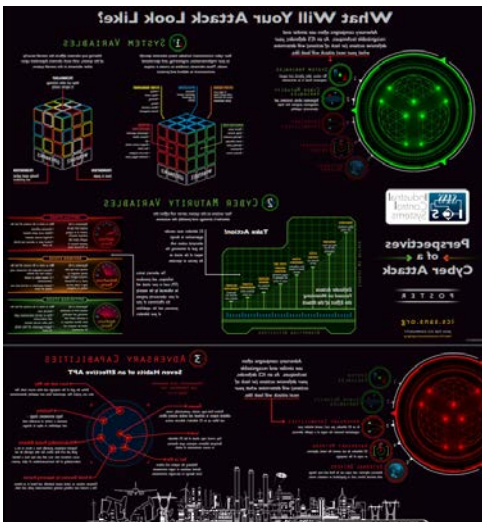


## • DNS

- <https://www.sans.org/security-resources/posters/all>

## Cyber Safe Work

<https://cybersafework.com/free-security-posters/>



# Components of a Cybersecurity Program

- **Vulnerability Assessment**

- Do you evaluate at both the system and component level?
- Do you have a process in place for identifying your vulnerabilities?
- How do you determine your prioritization of these vulnerabilities?
- How often is the vulnerability assessment done?

- **Tools**

- National Vulnerability Database
  - <https://nvd.nist.gov/>
- Schweitzer Engineering Laboratories – Security Vulnerability Notification

# Components of a Cybersecurity Program

- **Patch Management - Baseline**

- How often do you look for security patches?
- Do you install or mitigate or ignore?
- Do you test or verify?
- Do you track a Baseline and compare before and after changes are made?

- **Tools**

- FoxGuard Solutions – Not Free
  - <https://foxguardsolutions.com/>



# Components of a Cybersecurity Program

- **Transient Cyber Assets, Removeable Media**

- What do you allow to be connected to your Cyber Systems?
- Do you have a process to scan removable media prior to connection?
- Do you allow vendors to connect their equipment or media?
- Are you a contractor?



# Components of a Cybersecurity Program



- **Change Management**

- Do you document changes to your systems?
- Is there an approval process?
- Is a baseline kept?
- Do you track approved and scheduled changes that were not done?

# Components of a Cybersecurity Program

- **Cyber Security Incident Response and Reporting**
  - Is this documented in your program?
  - Does it include thresholds for calling and contact information for IT personnel? Upper management? Legal? Public Relations? Police? FBI?
  - Do you have required reporting? (E-ISAC, NCCIC, .....)
  - Do you contact neighboring utilities?
- **Do you participate in:**
  - GridEx
  - DHS CyberStorm

# Components of a Cybersecurity Program

- **System Recovery**

- Does your plan include backing up relay configuration?
- Do you test your backup files/media?
- Are your backup file sets stored offline?
- Do you test your recovery plan?

# Components of a Cybersecurity Program

- **Information Protection**

- Do you identify documents and files as being CEII, BESCSI, or other classifications?
- Does your classification allow for exclusion from a FOIA request?
  - <https://www.ferc.gov/legal/ceii-foia.asp>
- Does your plan include the allowance or process used for sending classified information through email, mail, company truck?
- Does your plan include the destruction of classified documents?
- Does your plan include the reuse or disposal of systems that have classified information?

# Components of a Cybersecurity Program

- **Supply Chain**
  - Where is your equipment coming from?
  - What about the parts and software located within that equipment?
  - Will your supply be impacted by the Cronavirus?
  - How does the vendor or manufacturer support the equipment?
  - Are vulnerabilities handled?
- **NERC Standard: CIP-013-1 Cyber Security - Supply Chain Risk Management**
  - Becomes effective July 1, 2020
  - Only applicable to Medium and High impact BES Cyber Systems
  - NERC is reporting to FERC that it should also be for Low Impact and include additional equipment.

# NERC CIP-013

- Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;
- Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;
- Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;
- Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;
- Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).

<https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf>



# Area of Concern - Information Silos

- **What is an Information Silo?**
  - Is information held by separate groups or individuals with limited sharing to others.
- **Using Information Silos, you can isolate the controls to your network or equipment**
  - This makes it more difficult for attackers to reach them since Information Silos only communicate vertically, and typically attackers go across a network horizontally



# Area of Concern - IoT

- **What does IoT stand for?**
  - IoT refers to the “Internet of Things”
- **What is the Internet of Things?**
  - “The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.”
- **Why is this important with regards to cybersecurity?**
  - Phil Muncaster, a reporter for “Infosecurity” magazine, illustrates this point very well stating “Mirai-like attacks which take advantage of weak factory-default log-ins for such devices are increasingly common, conscripting IoT endpoints into botnets which can then be used to launch DDoS and other attacks, Kaspersky explained. Some attacks also exploit old unpatched vulnerabilities to hijack devices, it added.”<sup>1</sup>



# Free Information Sources

- National Institute of Standards and Technology - NIST

- National Vulnerability Database

<https://nvd.nist.gov/>

- Information Sharing and Analysis Centers -

<https://www.nationalisacs.org/member-isacs>

Electricity ISAC - <https://www.eisac.com/>

Information Technology ISAC - <https://www.it-isac.org/>

Multi-State ISAC - <https://www.cisecurity.org/ms-isac/>

- Cybersecurity and Infrastructure Security Agency - <https://www.cisa.gov/>

- National Cybersecurity And Communications Integration Center

<https://www.us-cert.gov/nccic>

- Industrial Control Systems

<https://www.us-cert.gov/ics>



# Information Sharing and Analysis Centers



## North Carolina Information Sharing and Analysis Center

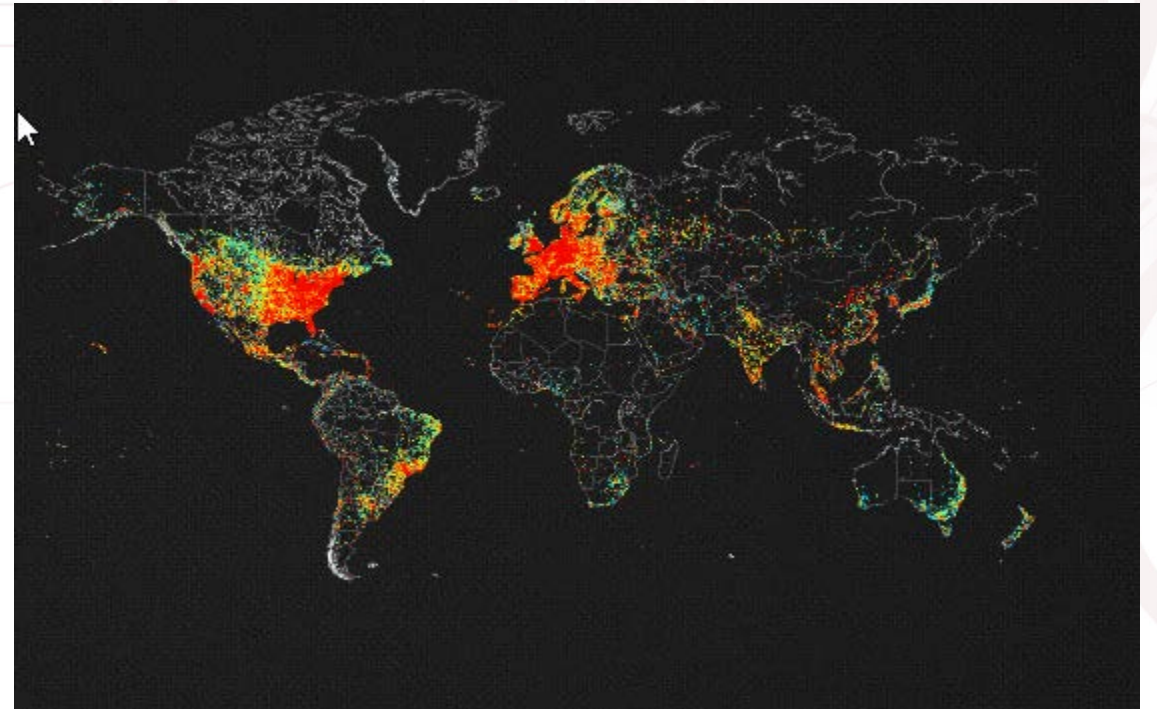
<https://www.ncsbi.gov/NCISAAC>



# Tools at a Glance

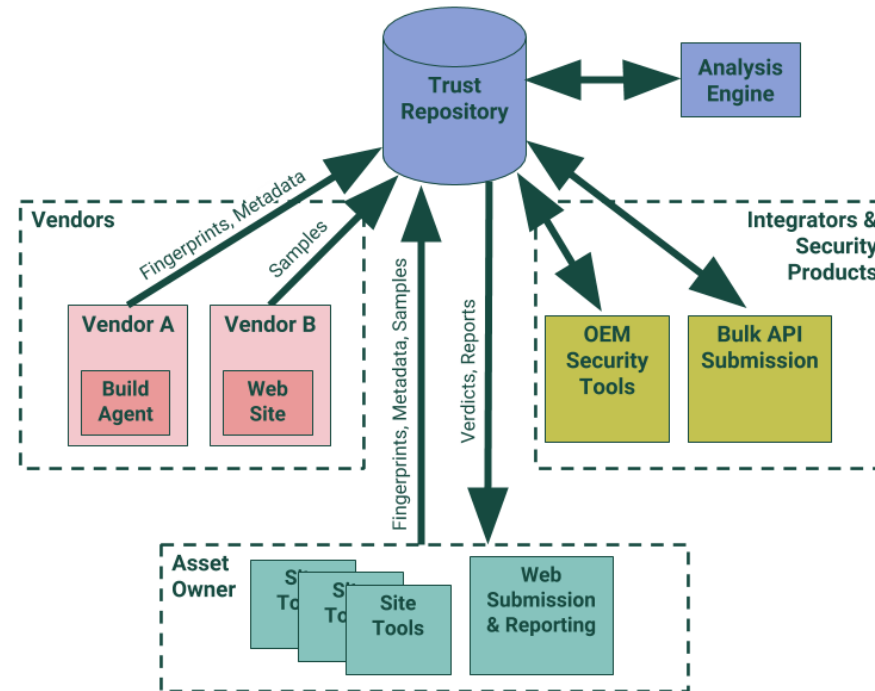
- **Shodan**  
Search tool for Internet-connected devices.

<https://www.shodan.io/>  
<https://beta.shodan.io/>



# Tools at a Glance

- aDolus FACT
  - Validates the integrity of software including patches



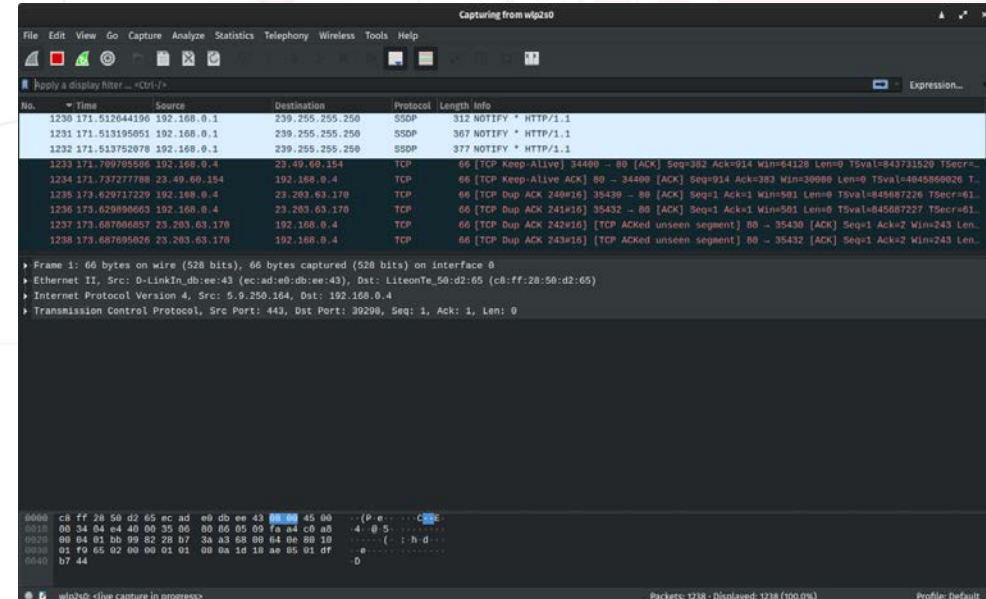
<https://www.adolus.com/>

# Tools at a Glance

- Wireshark (Packet Sniffers)

Wireshark® is a network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network

- <https://www.wireshark.org/>



By The Wireshark team  
Screenshot: Vulphere - Self-taken; derivative work, GPL,  
<https://commons.wikimedia.org/w/index.php?curid=81692859>

# Free Tools (cont.)

## Nmap (Network/Protocol Scanner)

- Nmap ("Network Mapper") is a free and open source ([license](#)) utility for network discovery and security auditing.

```
# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
|_ ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_ 2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp    open      http         Apache httpd 2.2.14 ((Ubuntu))
|_ http-title: Go ahead and ScanMe!
646/tcp   filtered  ldp
1720/tcp  filtered  H.323/Q.931
9929/tcp  open      nping-echo   Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
[Cut first 10 hops for brevity]
11 17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

<https://nmap.org/>

# Tools at a Glance

- Forensic Tool Kit (FTK)

From Wikipedia:

This is a computer forensics software made by [AccessData](#). It scans a hard drive looking for various information. It can, for example, locate deleted emails and scan a disk for text strings to use them as a password dictionary to crack encryption.

Includes FTK Imager which creates an image of a



# Tools at a Glance

## Snort

Snort is an open source network intrusion prevention system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more.

Snort has three modes of operation: sniffer, packet logger, and network intrusion detection.

Snort (IDS/IPS) (Windows and Linux) [https://www](https://www.snort.org)



# Tools at a Glance

## Nikto

Nikto is an open-source web server scanner. It will perform a comprehensive array of tests against web servers, testing for multiple items including over 6700 potentially dangerous files and programs. The tool will check for outdated versions of over 1250 servers and identify version-specific issues on over 270 servers. It can also check server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software.

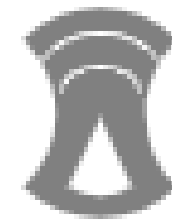


<https://cirt.net/Nikto2>

# Tools at a Glance

## Kismet

Kismet is a open source network detector, packet sniffer, and intrusion detection system for wireless LANs. It will work with any wireless card which supports raw monitoring mode and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic. The tool can run under Linux, FreeBSD, NetBSD, OpenBSD, and OS X. There is unfortunately very limited support for Windows mainly because only one wireless network adapter for Windows supports monitoring mode.



**Kismet**

<https://www.kismetwireless.net/>

# Tools at a Glance

## Autopsy

Autopsy was designed to be an end-to-end platform with modules that come with it out of the box and others that are available from [third-parties](#). Some of the modules provide:

[Timeline Analysis](#) - Advanced graphical event viewing interface (video tutorial included).

Hash Filtering - Flag known bad files and ignore known good.

[Keyword Search](#) - Indexed keyword search to find files that mention relevant terms.

[Web Artifacts](#) - Extract history, bookmarks, and cookies from Firefox, Chrome, and IE.

Data Carving - Recover deleted files from unallocated space using [PhotoRec](#)

Multimedia - Extract EXIF from pictures and watch videos.

Indicators of Compromise - Scan a computer using [STIX](#).

[\(Yes. This is directly from their website.\)](#)

<http://www.sleuthkit.org/autopsy/>



# Questions?





*The energy behind public power*

[www.electricities.com](http://www.electricities.com)

## **FOLLOW US ON SOCIAL MEDIA:**



@ncpublicpower



[facebook.com/Electricities](https://facebook.com/Electricities)



@ElectriCitiesNC