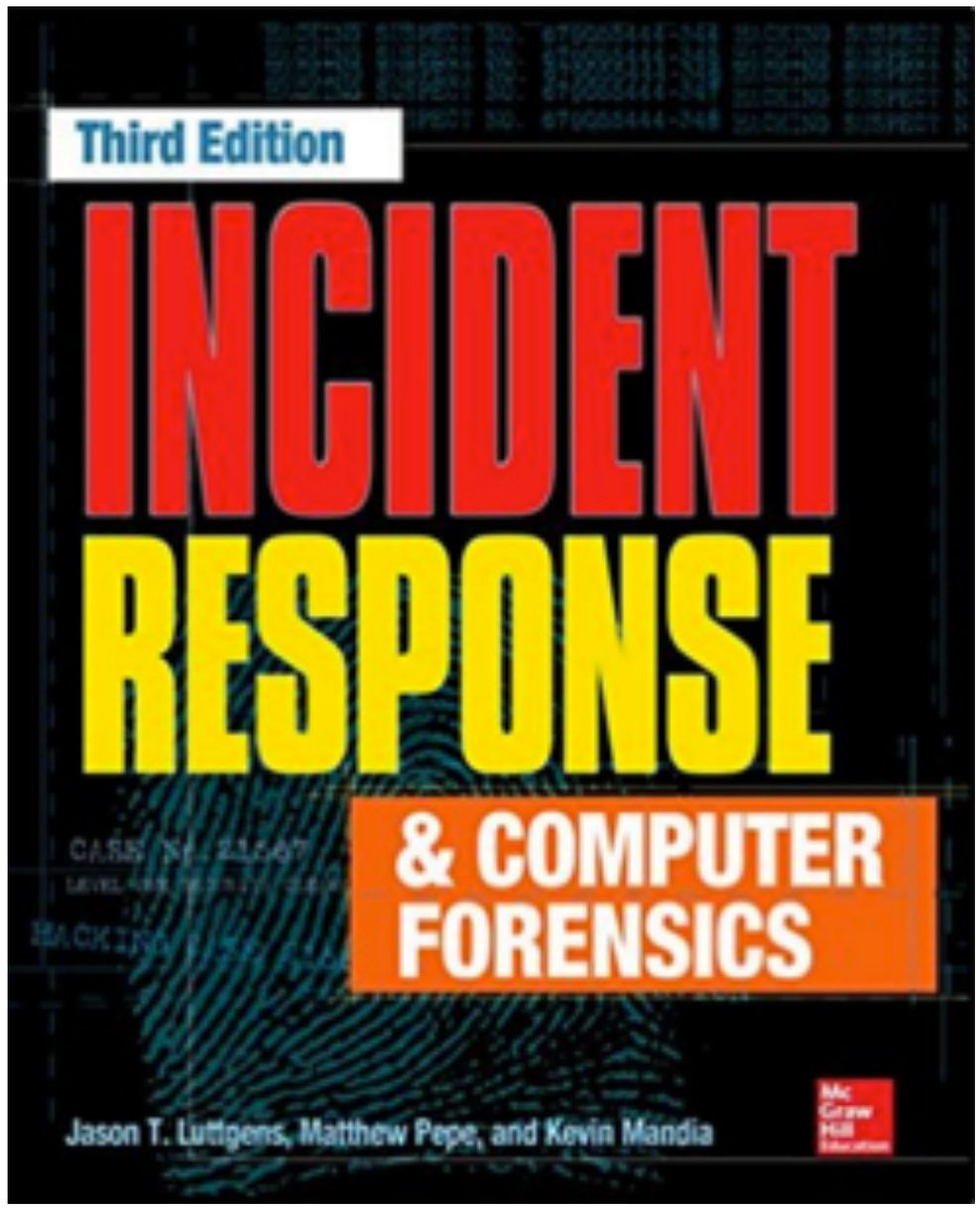
CNIT 152: Incident Response



3 Pre-Incident Preparation

Updated 9-9-2021

Questions During an Incident

- **What exactly happened? What is the damage and how did the attackers get in?**
- **Is the incident ongoing?**
- **What information was stolen or accessed?**
- **What resources were affected by the incident?**
- **What are the notification and disclosure responsibilities?**
- **What steps should be performed to remediate the situation?**
- **What actions can be taken to secure the enterprise from similar incidents?**

Three Areas of Preparation

- **Preparing the organization**
- **Preparing the IR team**
- **Preparing the infrastructure**

Preparing the Organization

Challenges

- **Identifying risk**
- **Policies that promote a successful IR**
- **Working with outsourced IT**
- **Thoughts on global infrastructure issues**
- **Educating users on host-based security**

Identifying Risk: Assets

- **Corporate reputation**
- **Confidential business information**
- **Personally identifiable information**
- **Payment account data**

Identifying Risk: Exposures

- **Unpatched web servers**
- **Internet-facing systems**
- **Disgruntled employees**
- **Untrained employees**

Identifying Risk: Threat Actors

- **Who can actually exploit these exposures**
  - **Anyone from the Internet**
  - **Physical access to building**
  - **Physically within a secure area**

Policies that Promote Successful IR

- **Acceptable Use Policy**
- **Security Policy**
- **Remote Access Policy**
- **Internet Usage Policy**

Working with Outsourced IT

- **Challenges may include**
  - **Red tape delays requesting work**
  - **Additional costs**
  - **No vehicle to accomplish a task, such as getting log files for analysis**
- **Service Level Agreements are required for responsiveness to critical requests**

Global Infrastructure Issues

- **Large multinational organizations**
  - **Privacy and labor regulations may limit searches for indicators of compromise**
  - **Team coordination across many time zones**
  - **Data accessibility--large data sets such as disk images are difficult to efficiently transfer**

Educating Users on Host-Based Security

- **Common ways users are targeted**
- **Proper response to suspected incidents**
  - **Specific contact person**
  - **Don't attempt an amateur investigation, which may destroy evidence**
- **Server software installed by users, such as FTP, can jeopardize the organization's security**

3a

Preparing the IR Team

Defining the Mission

- **Respond to all security incidents or suspected incidents using an organized, formal investigative process.**
- **Conduct a complete impartial investigation.**
- **Quickly confirm or dispel whether an intrusion or security incident actually occurred.**
- **Assess the damage and scope of an incident.**
- **Control and contain the incident.**
- **Collect and document all evidence related to an incident.**
- **Select additional support when needed.**

Defining the Mission

- **Protect privacy rights established by law and/or corporate policy.**
- **Provide a liaison to proper law enforcement and legal authorities.**
- **Maintain appropriate confidentiality of the incident to protect the organization from unnecessary exposure.**
- **Provide expert testimony.**
- **Provide management with recommendations that are fully supported by facts.**

Communications Procedures

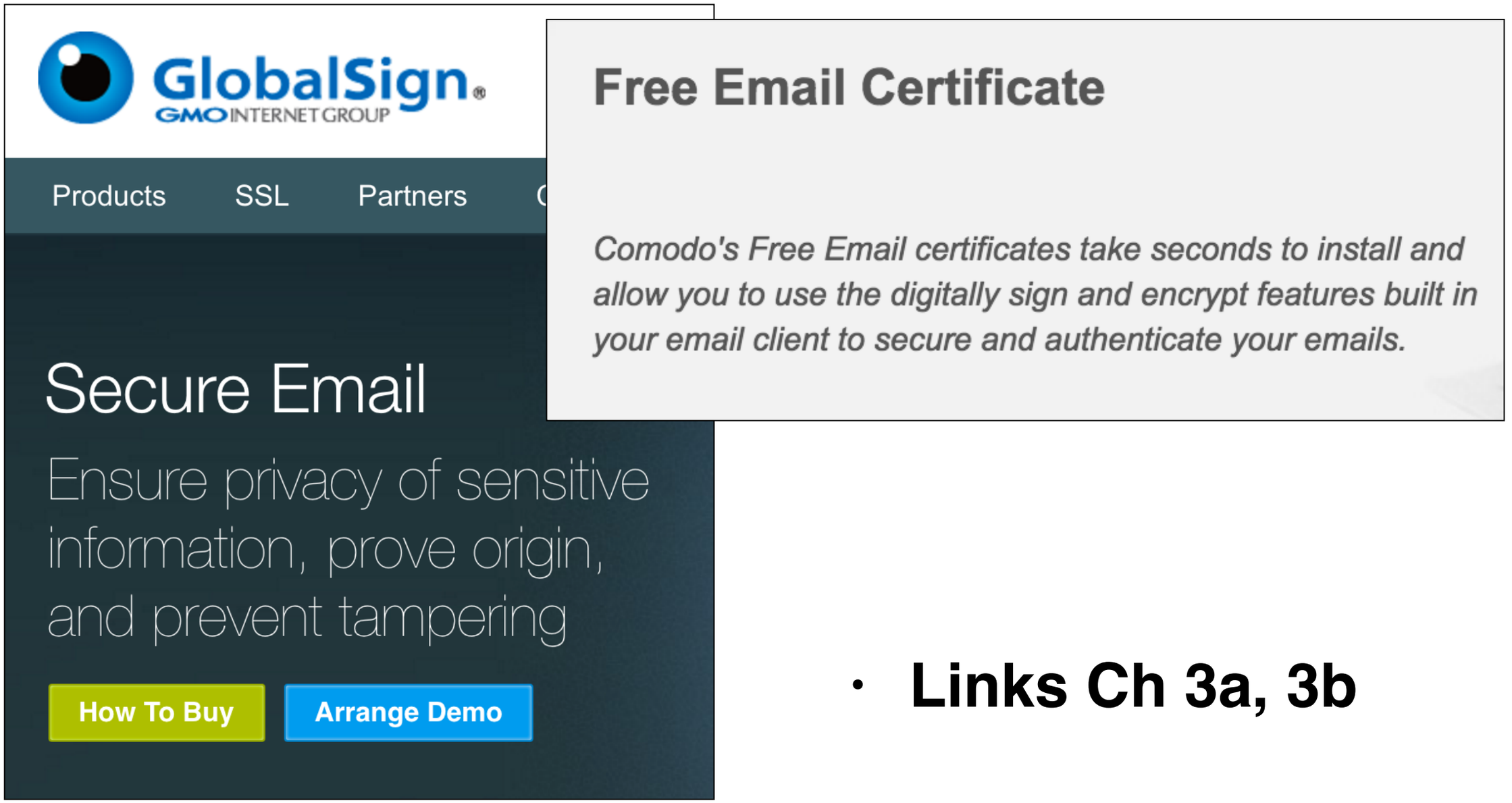
- **Your legal counsel may want to be included on certain communications to ensure that the information is not discoverable**

CONFIDENTIALITY NOTE: This email message contains information which may be privileged, confidential and/or protected from disclosure. The information is intended only for the use of the individual or entity named above. If you think that you have received this message in error, please email the sender then delete the email from your computer system and destroy any hardcopies of the email. If you are not the intended recipient any dissemination, distribution or copying is strictly prohibited.

Internal Communications

- **Attackers often monitor email to see if they have been detected**
- **Encrypt email with S/MIME or PGP**
- **Label documents and communications as recommended by your legal counsel**
- **Monitor conference call participation**
- **Use case numbers or project names to refer to an investigation**
- **Adjust emails from IDS systems and other devices not to disclose sensitive information**

S/MIME Certificates



- **Links Ch 3a, 3b**

Communicating with External Parties

- **Often required by governance and legislation**
- **Incident disclosure language in contracts**
- **Use approved channels, such as public relations or legal office**

Deliverables

Name	Purpose	Delivery Target
Case Status Report	Update stakeholders on progress of an individual case.	Recurring: Daily or as required
Live Response Report	Document findings from initial live response triage of a single system.	Draft: Within one business day Final: Within two business days
Forensic Examination Report	Document the detailed findings from forensic analysis performed on an item of evidence.	Draft: Within four business days Final: Within six business days
Malware Analysis Report	Document the findings from analysis of suspected malicious software.	Draft: Within three business days Final: Within five business days
Intrusion Investigation Report	Consolidate all reports and findings related to a single incident and create a high-level executive summary.	Draft: Within five business days of completion of the investigation Final: Within eight business days of completion of the investigation

Training the IR Team

- **Carnegie Mellon**
- **Purdue**
- **Johns Hopkins**
- **SANS**

Hardware to Outfit the IR Team

- **Data protection with encryption**
  - **Permanent, internal media (SSDs and hard disks)**
    - **Full-disk encryption (FDE) like TrueCrypt or McAfee Endpoint Encryption**
    - **Hardware-based FDE; Self-Encrypting Drive (SED)**
- **External media (thumb drives, USB hard disks or SSDs, external SATA drives)**
  - **TrueCrypt is a common solution**
  - **TrueCrypt is dead, replaced by VeraCrypt (links Ch 3c, 3d)**

Forensics in the Field

- **Laptop computer with**
  - **As much RAM as possible**
  - **The fastest CPU possible**
  - **I/O buses -- eSATA, Firewire 800, USB 3.0**
  - **Screen: large and high resolution**
  - **Large and fast internal storage drives**
  - **Portable and under warranty**

Forensics at the Office

- **Dedicated forensics lab**
  - **Systems with write-blockers**
  - **Secure storage for original material with written evidence-handling policies**
  - **Fresh, clean virtual analysis machines with forensic tools installed**
  - **Analysts work on copies of the data, never on original data**

Shared Forensics Equipment

- **Several write-blocking kits that allow PATA, SAT, SCSI, and SAS (Serial Attached SCSI)**
- **Stand-alone disk duplication and imaging systems**
- **Write blockers for all media interface types you expect to encounter**
- **Mobile device acquisition systems**
- **Assorted cables and adaptors**

Shared Forensic Equipment

- **Large external hard drives for evidence storage and for managing working copies of data**
- **Digital cameras for documenting evidence**
- **Blank CDs and DVDs**
- **Network switches and cabling**
- **Power strips and cables**
- **I/O bus cables—Firewire, eSATA, USB**
- **Computer maintenance tools such as screwdrivers, Torx bits, spudgers, and other specialized case-opening tools.**

Network Monitoring Platforms

- **For ad-hoc monitoring, a laptop similar to the one for on-site forensic work (with a built-in UPS)**
- **Most often, use a 1U rack-mount system**
  - **12-16 GB of RAM, high-end CPU, storage with enough speed and capacity to hold incoming data at 80% of line speed**
  - **Separate network port for management**

Network Monitoring Projects

Security Onion securityonion.blogspot.com
Network Security Toolkit networksecuritytoolkit.org
Easy-IDS skynet-solutions.net

Software for the IR Team

- **"Forensically Sound" software**
  - **Many people think a tool is approved by courts, such as EnCase, but any software may be used if the court accepts it**

Daubert Standard

- **For admissibility of scientific evidence**

  - **Has the scientific theory or technique been empirically tested?**
  - **Has the scientific theory or technique been subjected to peer review and publication?**
  - **Is there a known or potential error rate? Do standards that control the technique's operation exist?**
  - **Is there a general acceptance of the methodology or technique in the relevant scientific community?**

Additional Tests

- **Has the technique been created for a purpose other than litigation?**
- **Does the expert sufficiently explain important empirical data?**
- **Is the technique based on qualitatively sufficient data?**
- **Is there a measure of consistency to the technique's process or methods?**
- **Is there a measure of consistency to the technique's process or methods as applied to the current case?**
- **Is the technique represented in a body of literature?**
- **Does the expert possess adequate credentials in the field?**
- **How did the technique used differ from other similar approaches?**

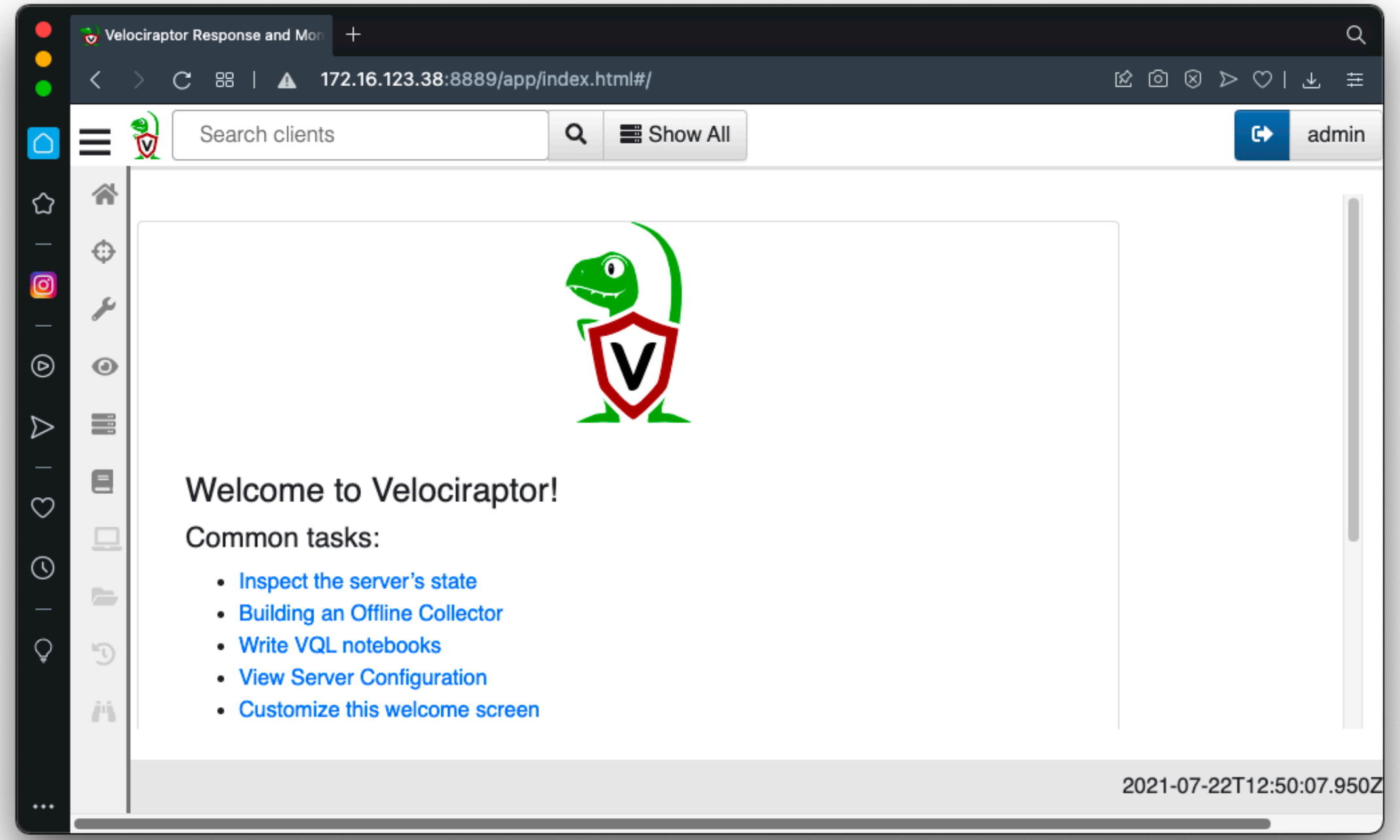
Software Used by IR Teams

- **Boot disks or USB sticks**
  - **Such as Kali, CAINE, or Helix**
- **Operating Systems (all common types, virtualized)**
- **Disk imaging tools (approved by NIST, link Ch 3h)**
- **Memory Capture and Analysis**

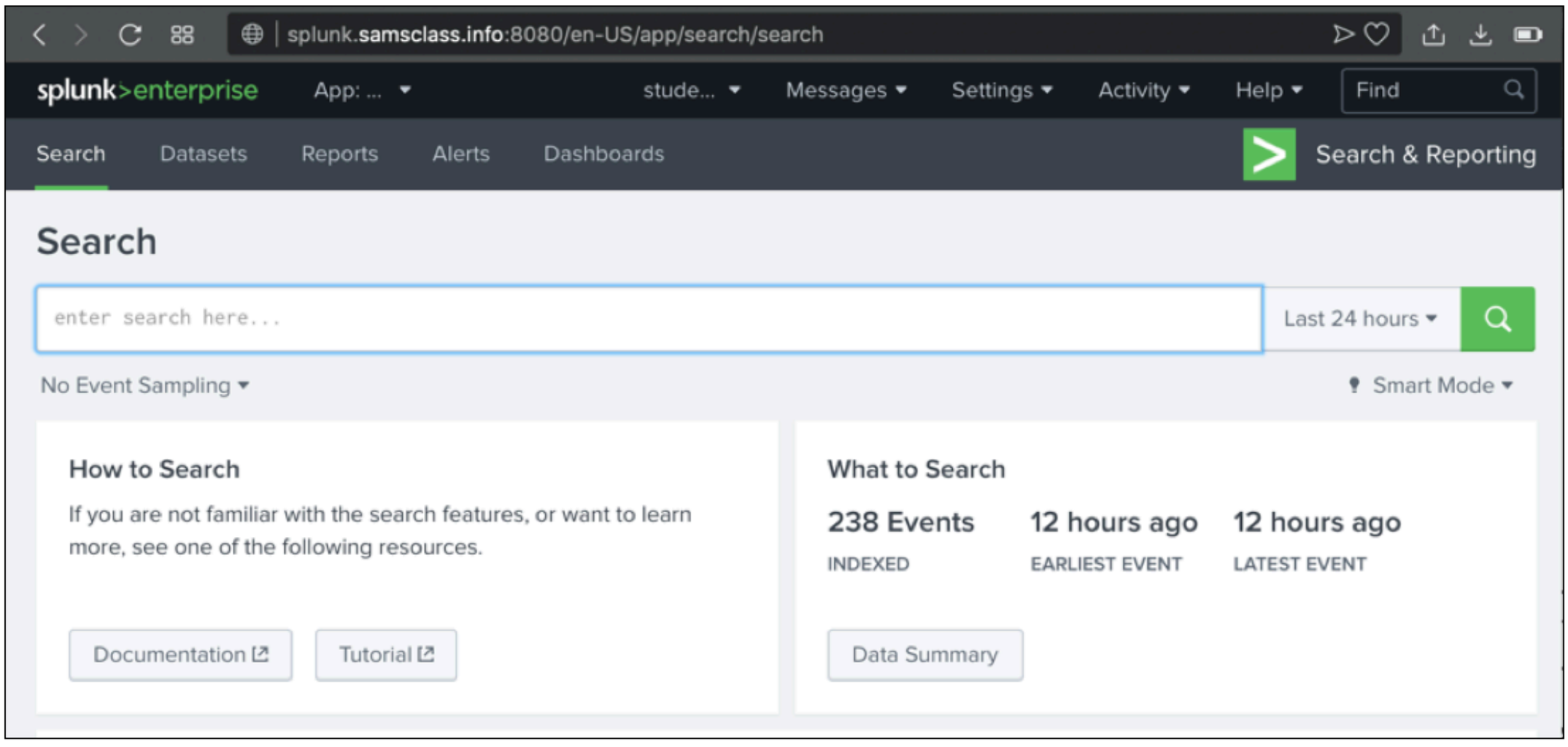
Software Used by IR Teams

- **Live response capture and analysis**
- **Indicator creation and search utilities**
- **Forensic examination suites**
  - **Like EnCase, FTK, or SleuthKit and Autopsy**
- **Log analysis tools**

Live Response: Velociraptor

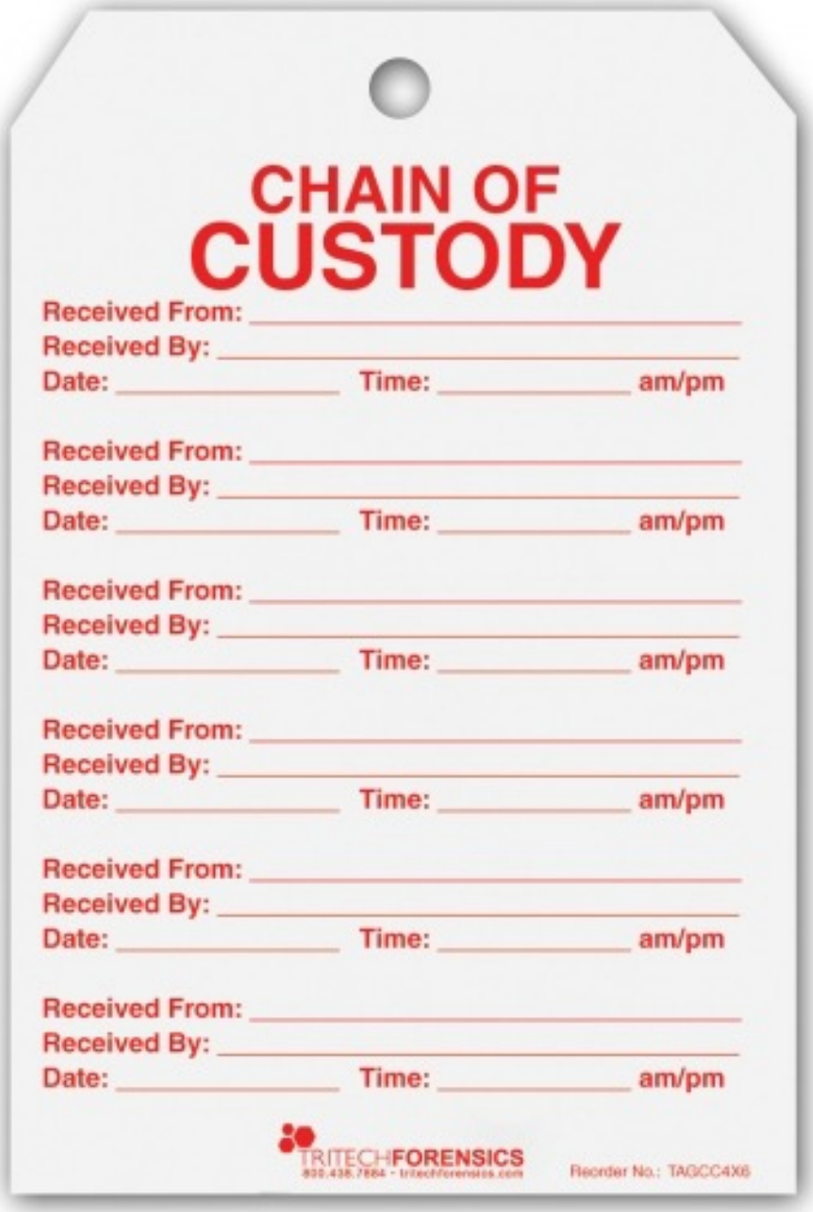


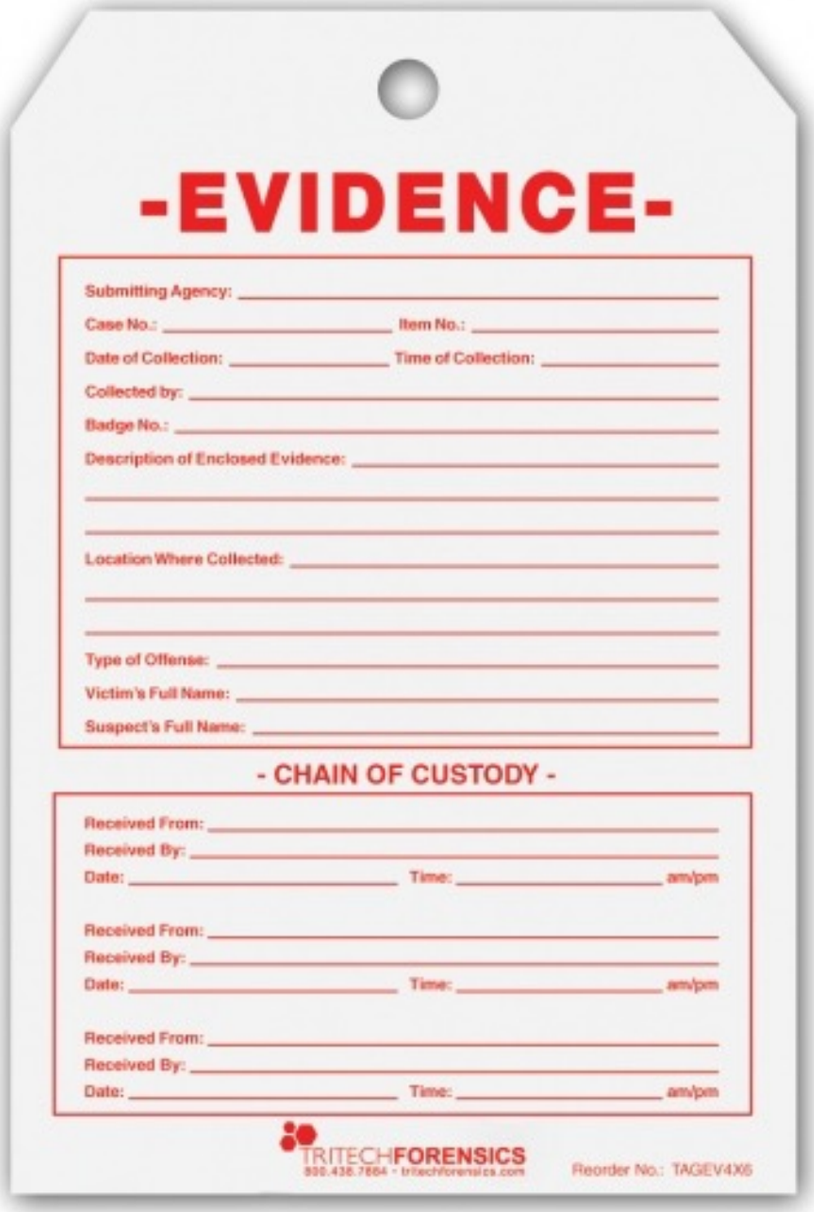
Log Analysis: Splunk



Documentation: Evidence Handling

- **Strict procedures to maintain integrity with *positive control***
  - **Evidence must be always under direct supervision, or secured in a controlled container, such a safe**
- **Evidence must be shipped via a traceable carrier, packaged in a tamper-evident manner, and protected from the elements**
- **Cryptographic hash value such as MD5**

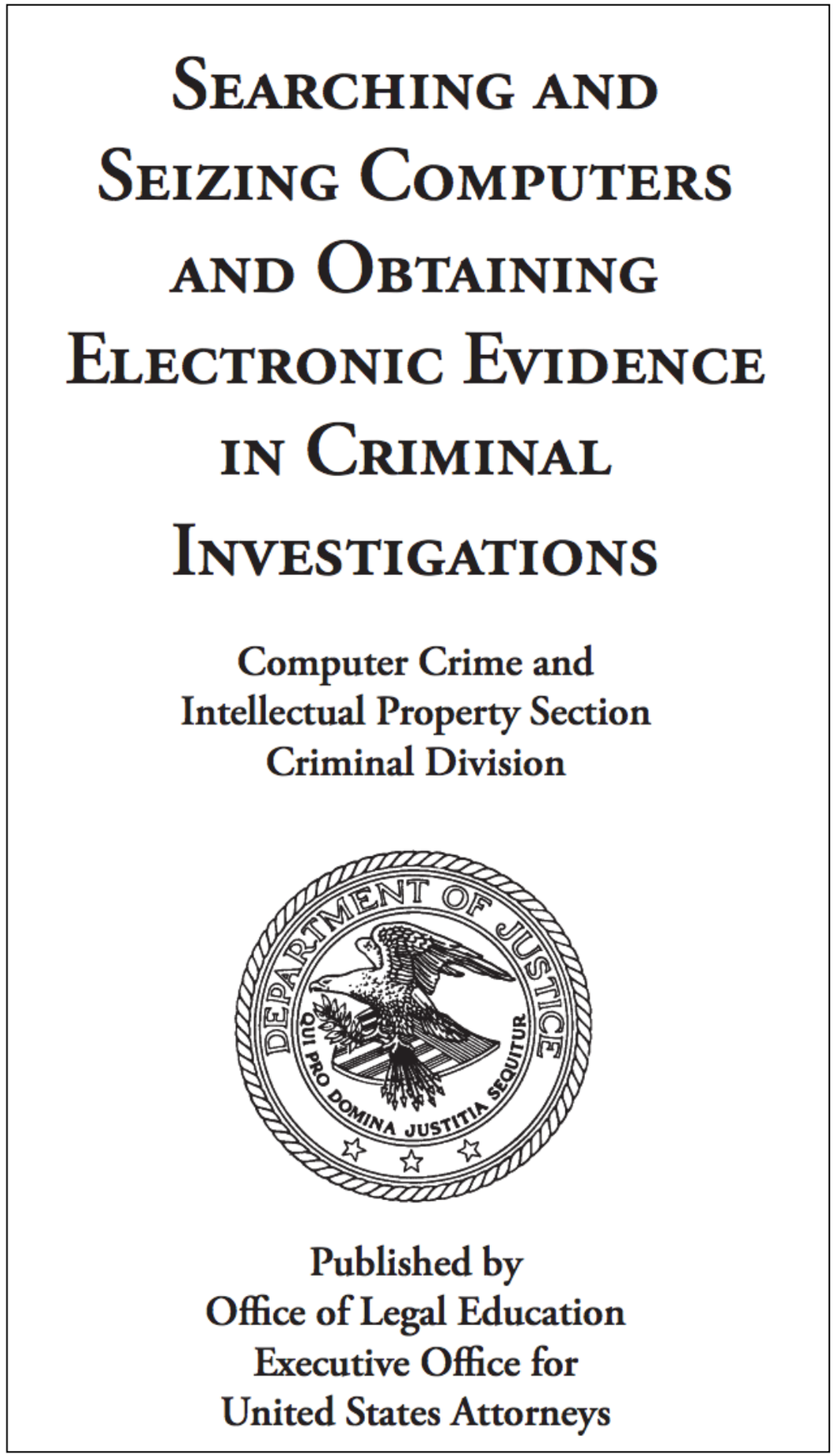




- **From link Ch 3i**

Evidence Handling

- **Link Ch 3j, 3k**



SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS

Computer Crime and
Intellectual Property Section
Criminal Division

DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR

Published by
Office of Legal Education
Executive Office for
United States Attorneys

Documentation:
Internal Knowledge Repository

- **Ticketing or case management system holds knowledge about a specific case**
- **Knowledge repository contains information relevant to many cases**
  - **Logically organized and searchable**

3b

Preparing the Infrastructure for Incident Response

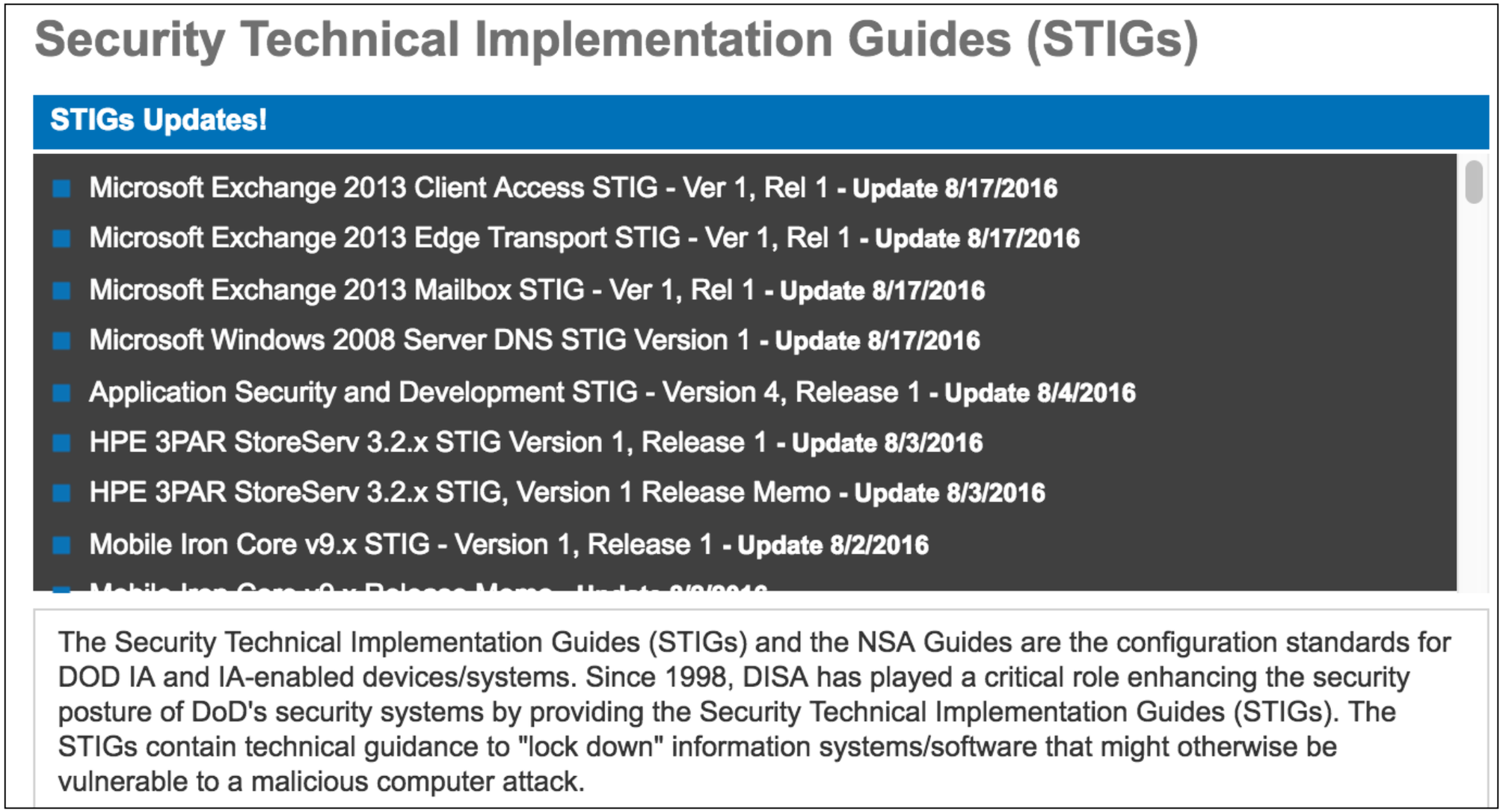
Problem Areas

- **Computing device configuration**
  - **Asset management**
  - **Performing a survey**
  - **Instrumentation**
  - **Additional steps to improve security**
- **Network configuration**
  - **Network segmentation and access control**
  - **Documentation**
  - **Instrumentation**
  - **Network services**

Computing Device Configuration

- **Many organizations focus attention on the systems they regard as important**
- **But attackers often use noncritical systems to base their attacks**
- **Two steps:**
  - **Understand what you have**
  - **Improve and augment**
    - **Log settings, antivirus, HIPS, etc.**

Host Hardening



Security Technical Implementation Guides (STIGs)

STIGs Updates!

- Microsoft Exchange 2013 Client Access STIG - Ver 1, Rel 1 - **Update 8/17/2016**
- Microsoft Exchange 2013 Edge Transport STIG - Ver 1, Rel 1 - **Update 8/17/2016**
- Microsoft Exchange 2013 Mailbox STIG - Ver 1, Rel 1 - **Update 8/17/2016**
- Microsoft Windows 2008 Server DNS STIG Version 1 - **Update 8/17/2016**
- Application Security and Development STIG - Version 4, Release 1 - **Update 8/4/2016**
- HPE 3PAR StoreServ 3.2.x STIG Version 1, Release 1 - **Update 8/3/2016**
- HPE 3PAR StoreServ 3.2.x STIG, Version 1 Release Memo - **Update 8/3/2016**
- Mobile Iron Core v9.x STIG - Version 1, Release 1 - **Update 8/2/2016**

The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

- **Link Ch 3l**

Asset Management

- **Need information about systems**
  - **Date provisioned**
  - **Ownership and Business Unit**
  - **Physical location**
  - **Contact information**
  - **Role or services**
  - **Network configuration**

Performing a Survey

- **Operating systems (Windows, Mac OS X, Linux, HP-UX)**
- **Hardware (laptops, desktops, servers, mobile devices)**
- **Networking technologies (switches, wireless access points, firewalls, IDS, proxies)**
- **Network diagram**
- **Security software (AV, HIPS, whitelisting)**
- **IT management software (patch, configuration, and asset management, performance monitoring)**
- **Endpoint applications (word processing, graphics, engineering, Internet browsers)**
- **Business applications (time keeping, document management, payment processing)**

Passwords

- **Attackers often obtain hundreds of thousands of passwords, by hash dumps of domain controllers**
- **Including service accounts**
  - **Often hard-coded into back-office systems and applications**
- **Same local administrator account on all systems**

Services

- **Run in the background**
- **Service accounts have "Log on as a service" rights**

Services (Local)

Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local System
AllJoyn Router Service	Routes AllJo...		Manual (Trig...	Local Service
App Readiness	Gets apps re...		Manual	Local System
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...	Running	Manual (Trig...	Local System
Application Layer Gateway Service	Provides su...		Manual	Local Service
Application Management	Processes in...	Running	Manual	Local System
AppX Deployment Service (AppXSVC)	Provides inf...		Manual	Local System
ASP.NET State Service	Provides su...		Manual	Network Service
Auto Time Zone Updater	Automatica...		Disabled	Local Service
Background Intelligent Transfer Service	Transfers fil...	Running	Automatic (D...	Local System

Instrumentation

- **Software metering**
  - **Compliance with licensing**
  - **Usage records**
- **Performance monitoring**
- **AV or host-based firewalls**
- **Event, error, and access logs**
  - **Centralized system is very helpful**

Centralized Logging Systems

- **Free**
  - **ELK, ELSA, Snare**
- **Commercial**
  - **Splunk, ArcSight, RSA's EnVision**

RSA ENVISION ES 560

- **Sustained Events/Second:** 500 EPS
- **Max Devices per Appliance:** 100
- **Simultaneous RSA Users:** 6
- **Storage:** 300 GB Internal
- **Virtualized Appliance:** Yes

Retention

- **Retain log data for at least a year**
  - **Required by PCI-DSS**

What to Log on Windows

- **Log-on and log-off events**
- **User and group management**
- **Process creation and termination**
- **Increase local storage for each event log to 100 MB or 500 MB**
- **Forward all events to centralized logging system**

What to Log on Unix

- **Enable process accounting**
- **increase local storage**
- **Forward all events to a centralized logging system**

What to Log from Applications

- **Web server, proxy, and firewall logs**
- **Database, email, DHCP, AV, IPS/IDS**
- **DNS query logging**
- **Custom applications**

Antivirus and Host Intrusion Prevention Systems

- **Log events to a central server**
- **Don't delete malware on detection**
  - **Quarantine it to a central location: preserves evidence**
- **Don't automatically transmit suspicious files to a vendor**
  - **May contain sensitive data like proxy settings or credentials**
  - **May alert the attacker that they've been caught**

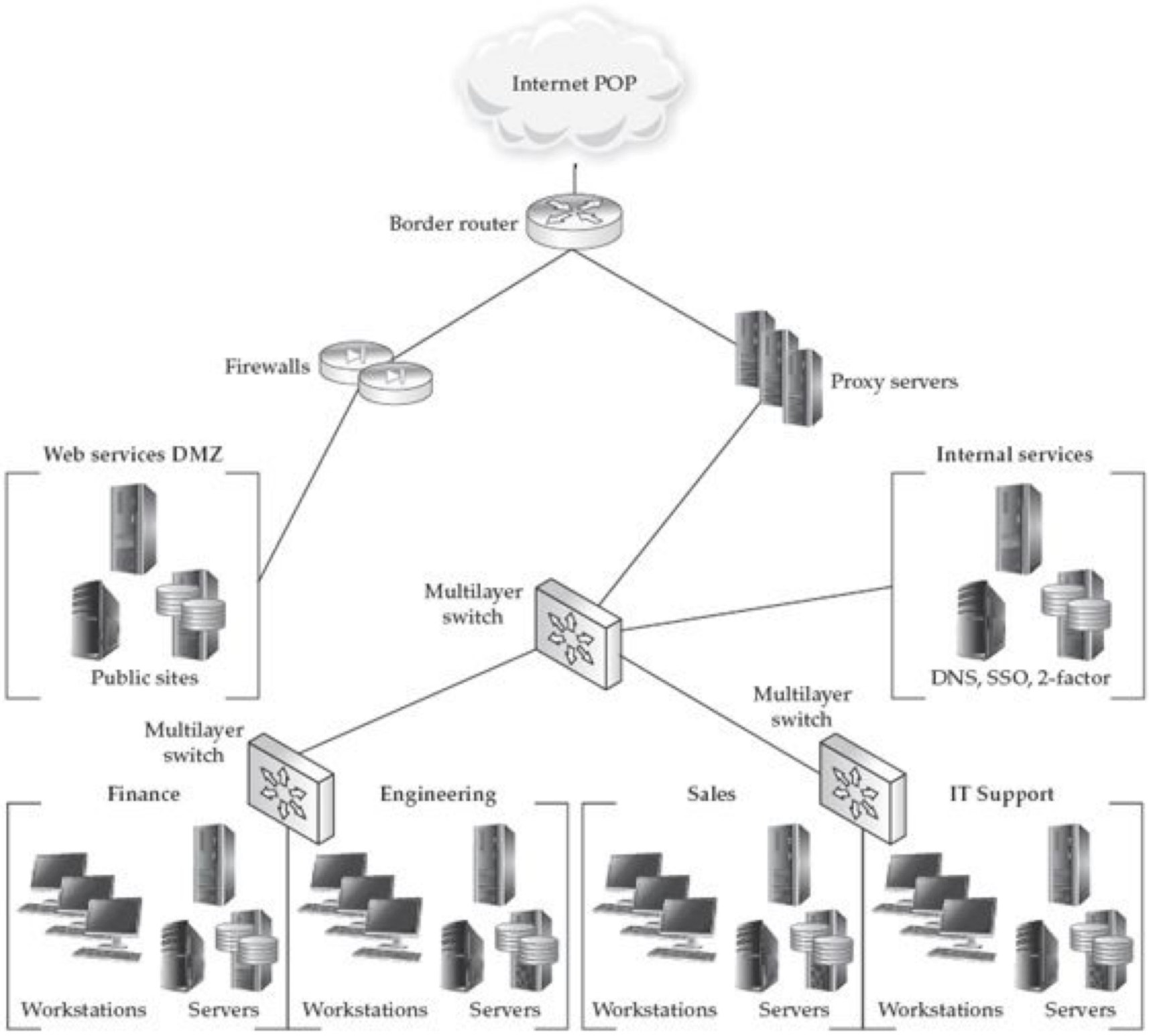
Investigative Tools

- **Can search your environment for artifacts like malware or attacker tools**
  - **AccessData Enterprise**
  - **Guidance Software EnCase Enterprise**
  - **Mandiant Intelligent Response**
  - **Homegrown solution using shell scripts and Windows Management Instrumentation (WMI)**

Additional Steps to Improve Security

- **Establish a patching solution for both operating systems and applications.**
- **Consider the use of two-factor authentication, and enforce good password complexity.**
- **Remove local administrative access from users.**
- **Ensure systems have firewall and AV solutions deployed and configured appropriately.**
- **Decommission end-of-life systems.**
- **Establish a configuration management system.**
- **Consider application whitelisting.**
- **Conform with DISA STIGs: iase.disa.mil/stigs.**
- **Follow NSA IA mitigation guidance: www.nsa.gov/ia/mitigation_guidance/index.shtml.**

Network Segmentation and Access Control



Controls

- **Traffic filtering at the sub-organization level**
- **Web, chat, and file transfer proxies**
- **Two-factor authentication for connections crossing significant borders**

Microsoft RPC
(Remote Procedure Calls)

- **Ports 135, 137, 138, 139, 445**

- **Once you allow access for file sharing, you get remote administration (psexec) over those same ports**

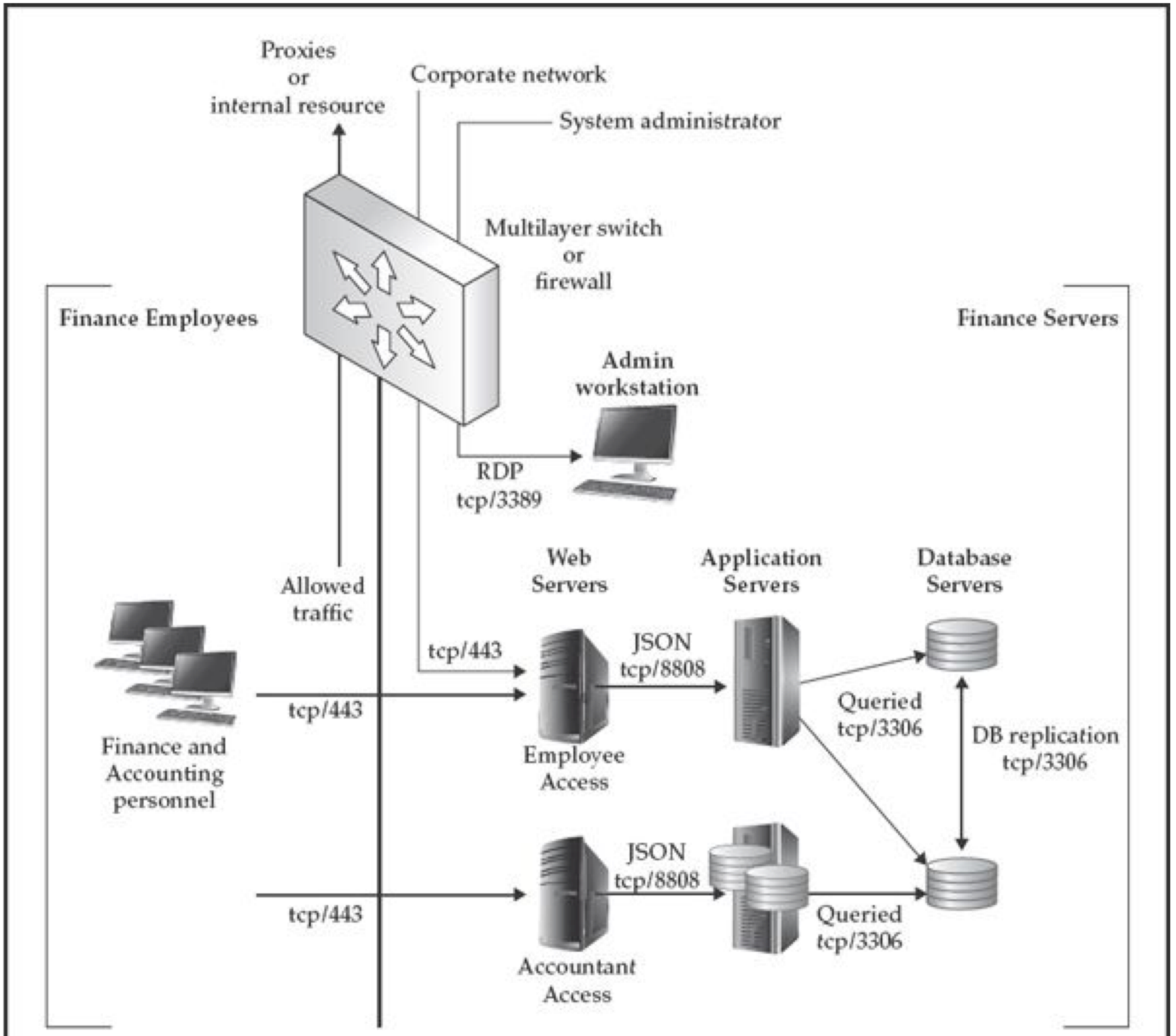


Figure 3-2. Network diagram of the Finance department

Access Control

- **Traffic between zones is carefully controlled**
- **Personnel in the Finance group can get email, Active Directory, and web traffic to proxies**
- **Connections to servers over HTTPS**
- **Servers are not allowed to send outbound traffic to the Internet**
- **For system management, administrator uses two-factor authentication to the specified administrative workstation (jump-box)**

Limiting Workstation Communication

- **Disallow traffic between ports on managed switches**
  - **Except to shared resources or another switch**
- **This can stop an infection from spreading**

Blackholes

- **Remove default routes from internal routers and switches**
- **Workstations and servers that require access to external resources must go through the authenticated proxy**
  - **Proxy logs can detect unusual traffic patterns**
- **Traffic to external IP addresses sent to a blackhole or a system for analysis**
  - **Can act as a simple early-warning system**

Honeypots

- **A waste of time**
- **Better to focus on defending your real assets**

Documentation

- **Network diagrams at various levels**
  - **Placement of network monitoring devices requires that information**
- **Device configurations (routers, firewalls, switches)**
  - **Change control can detect tampering**

Logging and Monitoring Devices

- **Firewalls**
- **Intrusion Detection Systems**
- **Full-content capture systems**
  - **Hardware network tap**
- **Netflow emitters (statistical traffic monitoring)**
- **Proxy servers**

Network Services

- **Configure DNS and DHCP services for extensive logging**
- **Retain the logs for at least a year**
- **Configure a DNS blackhole to redirect malicious traffic to a monitoring server**
  - **Links Ch 3q, 3r**

3c