Unit-III
Internet Forensic

Internet forensics

- Internet forensics relates to the examination of infrastructure out of one’s control,such as servers in other countries.
- Internet forensics applies to both investigations of crimes committed on the Internet and investigations of crimes committed with the Internet.
- computer intrusion, denial-of-service attacks, and bankfraud
- Identity theft, extortion, and money laundering

IF-3 crime scenes

- Adversary
- Victim
- Infrastructure
- Environment
- Computer network- osi ,tcp model
- Internet backbone-AS,BGP,RIP
- ISP

Domain Name Ownership Investigation

- Responsible for naming
- Set of hierarchically organized name servers
- Mapped to server & Managed by IANA
- Domain name consists of one or more alphanumeric strings separated by dots. The part at the far right is referred to as the top-level domain(TLD)
- TLDs has been restricted to relatively few, only national identifiers, such as. no, .se ,and. dk, and some generic namesl ike. com,.net,.org,and.info.

Domain Name Ownership Investigation

- Recently,it has become possible to acquire complete TLDs ,Ex:- .google.
- There are 7 different types of DNS records
- 16 root servers
- Delegation to servers

World Wide Web Threats

- Sem V NS
- Hacking and Illegal access
- Sem VI EH

Domain Name Ownership Investigation

- Domain Dossier tool generates **reports from public records** about domain names and IP addresses to help solve problems, investigate cybercrime, or just better understand how things are set up

- Owner’s contact information
- Registrar and registry information
- The company that is hosting a Web site
- Where an IP address is geographically located
- What type of server is at the address
- The upstream networks of a site and much more

Domain Name Ownership Investigation

- Entering an address
- Address lookup
- Domain Whois record
- Network Whois record
- DNS records
- Traceroute
- Service scan

- Every Dossier begins with a DNS lookup for what you entered:
- If you entered a domain name, it looks up IP addresses for the domain.
- If you entered an IP address, it does a “reverse” lookup to get associated domain names.

Domain Whois record

- The name of the registrant
- Contact information
- The date of the registration
- The date that the registration expires
- Authoritative DNS servers for the domain

Network Whois record

- The range of IP addresses in the assignment
- The name of the organization to which the addresses were assigned
- Contact information, including abuse contacts
- The date of the assignment

DNS records

- The entered domain (or the domain associated with the IP address you entered)
- Registered domain of the entered domain
- Canonical domain
- Zone apex for the canonical domain
- IP address domain (under in-addr.arpa or ip6.arpa)
- Zone apex for the IP address domain

- **Traceroute**
- **Service Scan**

Unit 4 syllabus

- **E-mail Forensics**: e-mail analysis, e-mail headers and spoofing, Laws against e-mail Crime, Messenger Forensics: Yahoo Messenger
- **Social Media Forensics**: Social Media Investigations
- **Browser Forensics**: Cookie Storage and Analysis, Analyzing Cache and temporary internet files, Web browsing activity reconstruction
- **Investigation, Evidence presentation and Legal aspects of Digital Forensics: Authorization to collect the evidence, Acquisition of Evidence, Authentication of the evidence, Analysis of the evidence, Reporting on the findings, Testimony, Report Writing for High-Tech Investigations**
- **Introduction to Legal aspects of Digital Forensics**: Laws & regulations, Information Technology Act, Giving Evidence in court, Case Study – Cyber Crime cases, Case Study – Cyber Crime cases.
- **Web browsing activity reconstruction**