RED HERRINGS
redherrings.app

COURSE PACK

Syllabus

Introduction to Digital Forensics

A 14-week undergraduate course: Windows artifacts, memory, network and mobile evidence, ending in a graded capstone.

Course code	[DEPT 000]
Term	[Term and year]
Instructor	[Name]
Contact	[Email]
Office hours	[Days, times, location or link]
Meeting pattern	[Days, times, room or lab]
Length	14 weeks, one lab per week
Discipline	Digital Forensics
Level	Undergraduate, second or third year
Prerequisites	Operating systems fundamentals and basic networking. No prior forensics.
Lab time	About 13 hours of hands-on work across the term
Prepared	2026-11-11

Bracketed fields are for the adopting instructor to complete. Everything else can be used as written. Every lab in this course generates a different variant of its case for each student, with an answer key verified against that student's own evidence; grading and the student portal run on the instructor's machine.

1. Course description

Students in this course learn digital forensics by doing it: they receive evidence, work it with the free tools examiners use on the job, and write up what they found. The first six weeks each isolate one Windows artifact family (removable devices, program execution, user files, persistence, event logs) and end by combining them into a timeline. A timed midterm applies all six to an insider theft. The second half widens the evidence to browser, cloud, memory, network and mobile sources, and the course closes with a timed capstone on a multi-host intrusion and a written investigation report. Every lab is a different variant of its case for every student, so there's no answer key to copy; each student has to read their own evidence.

2. Learning outcomes

On completing the course a student can:

1. Acquire and verify evidence, and keep a chain of custody.
2. Recover program execution, file, USB and persistence artifacts from a Windows system.
3. Build and defend a timeline from several artifacts.
4. Triage memory, network and mobile evidence with free tools.
5. Write an investigation report that states findings, cites artifacts and explains method.

3. Prerequisites and materials

Prerequisites

Operating systems fundamentals and basic networking. No prior forensics.

Software

All tools are free. One-run install scripts for each are on the Tools page of the product website.

Tool	Used for
Autopsy	disk image triage and file recovery
Registry Explorer	SYSTEM, SOFTWARE and NTUSER hives
EvtxECmd	Windows event logs to CSV
PECmd	Prefetch
LECmd	LNK shortcut files
JLECmd	jump lists
Volatility 3	memory images
Wireshark	packet captures
DB Browser for SQLite	browser and mobile databases
Timesketch	super-timelines (optional; a spreadsheet works)

Hardware

A laptop or lab workstation with 8 GB of RAM (16 GB for memory forensics weeks), 20 GB of free disk and permission to install the listed tools. Windows, macOS and Linux all work; some tools are Windows-only and run in a virtual machine elsewhere.

Evidence

Evidence is generated per student and handed out as a ZIP or through a private portal link each week. No textbook purchase is required; each week names its reading from the free references below.

Readings and references

No purchase is required. The texts below are free from their publishers, and each week names the part to read. Editions and addresses change; the title and publisher are the stable reference.

Title	Publisher	Use in this course
Guide to Integrating Forensic Techniques into Incident Response (SP 800-86) https://doi.org/10.6028/NIST.SP.800-86	NIST	The course spine for process: collection, examination, analysis, reporting.
Forensic Examination of Digital Evidence: A Guide for Law Enforcement https://nij.ojp.gov/library/publications/forensic-examination-digital-evidence-guide-law-enforcement	US National Institute of Justice	Chain of custody and documentation, weeks 1 and 14.
Windows Forensic Analysis poster https://www.sans.org/posters/	SANS Institute (free posters)	One page per artifact family; the map for weeks 1 to 6 and 8.
Windows security auditing: events to monitor https://learn.microsoft.com/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor	Microsoft Learn	Event id reference for week 5 and the midterm.
Eric Zimmerman's tools documentation https://ericzimmerman.github.io/	Eric Zimmerman	PECmd, LECmd, JLECmd, EvtxECmd, Registry Explorer and Timeline Explorer usage.
Autopsy user documentation https://sleuthkit.org/autopsy/docs/user-docs/	Sleuth Kit Labs	Disk image triage, weeks 1, 7 and 14.
Volatility 3 documentation https://volatility3.readthedocs.io/	Volatility Foundation	Memory forensics, weeks 10 and 11.
Wireshark User's Guide https://www.wireshark.org/docs/wsug_html_chunked/	Wireshark Foundation	Display filters and following streams, week 12.
Guidelines on Mobile Device Forensics (SP 800-101 Rev. 1) https://doi.org/10.6028/NIST.SP.800-101r1	NIST	Mobile data stores and extraction levels, week 13.
Open Textbook Library: digital forensics titles https://open.umn.edu/opentextbooks/	University of Minnesota	Search for current open, CC-licensed forensics texts to assign as background reading.

4. How a week runs

1. Each week has one lab built on a single case. Every student receives a different variant of that case: different names, hosts, timestamps and answers, generated from the same story.

2. Before the lab, read the briefing and the week's preparation notes, and confirm the listed tools open on your machine.

3. During the lab, work the evidence with the listed tools and record each answer with the artifact and method that proves it.

4. Submit through the student portal link for that week, or hand in the worksheet. Portal submissions are graded against your own answer key the moment you submit.

5. After release, review the walkthrough for your variant: where each answer was, and how it was found.

5. Assessment and grading

Component	Weight	Details
Weekly labs (12)	50%	Best 10 of 12 count. Auto-graded on submission; each lab is up to 20 questions on that week's case.
Midterm practical	20%	Week 7. A 75-minute timed exam in the portal on a full insider-theft case covering weeks 1 to 6.
Capstone practical	20%	Week 14. A 120-minute timed exam on a multi-host credential-theft intrusion.
Investigation report	10%	Due one week after the capstone. A written report on the capstone case, graded with the rubric below.

Grading scale

A	90 to 100
B	80 to 89
C	70 to 79
D	60 to 69
F	below 60

Timed assessments are graded on submission in the portal. Reports are graded with the rubric in section 8. Scores export to the institution's LMS from each week's job.

6. Course policies

Collaboration

Discussing tools and technique with classmates is encouraged. Answers aren't transferable: each variant has its own evidence and its own key, and a submission that matches another student's variant rather than your own is flagged by the collusion report and treated as academic misconduct.

Late work

Labs are due at the end of the week they're set. Late labs lose 10% per day for three days and aren't accepted after that. The lowest lab scores are dropped as stated in the assessment table, which covers illness and emergencies without paperwork for short absences.

Timed assessments

Timed exams run in the student portal with a fixed clock, shuffled question order and integrity logging (tab switches, full-screen exits and pastes are recorded). Arrive with your tools installed and tested.

Resubmission

One lab per term may be resubmitted within a week of feedback for up to 80% of full credit.

Evidence handling

Evidence files are synthetic. Treat them as you would real evidence anyway: verify hashes, work on copies, and document every step. That habit is assessed.

Accommodations

[Insert the institution's disability accommodation and extended-time statement. The portal supports per-student time extensions.]

Academic integrity

[Insert the institution's academic integrity statement.]

7. Schedule

One case per week. The mode and time budget are set when the course is generated; the deliverable is what the student hands in.

Wk	Topic	Case	Mode	Assessment
1	Evidence handling and the registry	First Look: USB Device History	Practice, about 33 min	Lab 1
2	Program execution	First Look: What Ran on This Machine	Practice, about 33 min	Lab 2
3	Files the user touched	First Look: Recent Files and Jump Lists	Practice, about 33 min	Lab 3
4	Persistence	First Look: What Runs at Startup	Practice, about 33 min	Lab 4
5	Windows event logs	First Look: Accounts and Services in the Logs	Practice, about 35 min	Lab 5
6	Timelines	First Look: Building a Timeline	Practice, about 37 min	Lab 6
7	Midterm practical	Insider Data Theft via USB	Timed exam, 75 min	Midterm 20%
8	Browser and download forensics	First Look: Suspicious Download	Practice, about 33 min	Lab 7
9	Data exfiltration	The Customer Export	Practice, about 80 min	Lab 8
10	Memory forensics	First Look: What's in Memory	Practice, about 37 min	Lab 9
11	Code injection in memory	Injected Code in Memory	Practice, about 119 min	Lab 10
12	Network forensics	First Look: Reading a Packet Capture	Practice, about 33 min	Lab 11
13	Mobile forensics	The Texts They Deleted	Practice, about 70 min	Lab 12
14	Capstone practical and report	Credential Theft and Lateral Movement	Timed exam, 120 min, with report	Capstone 20% + report 10%

Week by week

Each week below lists its objectives, the case and what it contains, what students should do beforehand, what they hand in, and a note for the instructor.

Week 1: Evidence handling and the registry

Objectives

• Explain acquisition, hashing and chain of custody.

• Read USBSTOR and device properties in a SYSTEM hive.

Case

First Look: USB Device History. Registry hives and a shortcut file. Work out which USB drive was plugged into the machine, when, and what was opened from it.

Practice, about 33 min · Up to 15 questions · Tools: Registry Explorer, RegRipper, LECmd

Reading

SP 800-86 sections 3.1 to 3.2 (collection) and the NIJ guide chapter on documenting the scene. SANS poster: USB devices.

Before the lab

Install Registry Explorer and Autopsy. Print the chain-of-custody form from the course materials.

Deliverable

Lab 1 answers in the portal and a completed chain-of-custody form for the evidence ZIP.

Instructor note

Spend the first half hour on hashing and the custody form before anyone opens a hive; it sets the standard for the term.

Week 2: Program execution

Objectives

• Interpret Prefetch and UserAssist.

• Tell a decoy execution from the real one.

Case

First Look: What Ran on This Machine. One user's execution artifacts. Test a user's claim that they never ran a program they downloaded.

Practice, about 33 min · Up to 15 questions · Tools: PECmd, Registry Explorer, LECmd

Reading

SANS poster: program execution (Prefetch and UserAssist). PECmd page in the Zimmerman docs.

Before the lab

Install PECmd. Read the program execution section of the SANS poster.

Deliverable

Lab 2 answers. For one question, a screenshot of the record that proves it.

Instructor note

Every variant plants a decoy execution with a similar name; the discussion of how students told them apart is the lesson.

Week 3: Files the user touched

Objectives
• Parse LNK files and jump lists.

• Recover a target path and its timestamps.

Case
First Look: Recent Files and Jump Lists. Shortcuts, jump lists and registry MRUs. Reconstruct what a departing employee opened, where each file lived, and when.

Practice, about 33 min · Up to 15 questions · Tools: JLECmd, LECmd, Registry Explorer

Reading
SANS poster: file and folder opening (LNK, jump lists). LECmd and JLECmd pages.

Before the lab
Install LECmd and JLECmd.

Deliverable
Lab 3 answers.

Instructor note
Have students compare LNK target timestamps with the file system; the mismatch is the point.

Week 4: Persistence

Objectives
• Enumerate Run keys, services and scheduled tasks.

• Rank persistence mechanisms by stealth.

Case
First Look: What Runs at Startup. A workstation keeps reinfecting itself after cleanup. Find what brings the malware back.

Practice, about 33 min · Up to 15 questions · Tools: Registry Explorer, RegRipper, PECmd

Reading
SANS poster: persistence. Microsoft Learn: Run and RunOnce keys, scheduled tasks.

Before the lab
Read the persistence section of the SANS poster: Run keys, services, scheduled tasks, WMI.

Deliverable
Lab 4 answers and a one-paragraph ranking of the persistence mechanisms found, most to least stealthy.

Instructor note
Ask for the ranking before revealing the key; it's the first judgment call of the course.

Week 5: Windows event logs

Objectives

• Read 4720, 4732, 7045 and 1102 events.

• Distinguish the acting account from the target account.

Case

First Look: Accounts and Services in the Logs. Exported event logs from one server. Find the account and service changes made overnight and who made them.

Practice, about 35 min · Up to 15 questions · Tools: Event Viewer, EvtxECmd

Reading

Microsoft events to monitor: 4720, 4732, 7045, 1102. EvtxECmd page.

Before the lab

Install EvtxECmd and Timeline Explorer. Skim the Microsoft events to monitor table for 4720, 4732, 7045 and 1102.

Deliverable

Lab 5 answers.

Instructor note

The acting-account versus target-account confusion in 4720 and 4732 catches most students; make it an explicit question in class.

Week 6: Timelines

Objectives

• Normalize timestamps across artifacts.

• Build and present a super-timeline.

Case

First Look: Building a Timeline. Two artifacts, one clock. Line up a browser download and a Security log to reconstruct the order things happened.

Practice, about 37 min · Up to 15 questions · Tools: Timesketch, EvtxECmd, DB Browser for SQLite

Reading

SP 800-86 section 3.3 (examination and analysis). Timeline Explorer page.

Before the lab

Choose a timeline tool: Timesketch, Timeline Explorer or a spreadsheet. Have weeks 1 to 5 output at hand.

Deliverable

Lab 6 answers and a one-page super-timeline of the week's case in one timezone.

Instructor note

A good checkpoint before the midterm: the timeline shows who can combine artifacts and who is still working one at a time.

Week 7: Midterm practical

Objectives
• Apply weeks 1 to 6 to a full insider-theft case under time.

Case
Insider Data Theft via USB. An engineer who has resigned is suspected of walking out with confidential files on a USB stick. Prove what was connected, what was copied, and when.

Timed exam, 75 min · Up to 20 questions · Tools: Autopsy, Registry Explorer, FTK Imager, PECmd, JLECmd, LECmd

Reading
Review weeks 1 to 6. No new reading.

Before the lab
Review weeks 1 to 6. Test every tool the night before; the clock doesn't stop for installs.

Deliverable
Midterm submitted in the portal within 75 minutes.

Instructor note
Run in exam mode with integrity logging. Release scores after the session so late sitters aren't tipped off.

Week 8: Browser and download forensics

Objectives
• Trace a download from history to disk.

• Read browser SQLite stores.

Case
First Look: Suspicious Download. One Chrome profile. Work out what the user searched for, where they went, and what they downloaded.

Practice, about 33 min · Up to 15 questions · Tools: DB Browser for SQLite, Browser History Viewer

Reading
SANS poster: browser usage. Autopsy user docs: web artifacts.

Before the lab
Install DB Browser for SQLite. Locate the browser history database on your own machine first.

Deliverable
Lab 7 answers.

Instructor note
Have students find their own download history before the lab; the structure then feels familiar.

Week 9: Data exfiltration

Objectives
• Correlate browser, LNK and email evidence.

• Prove which file left and when.

Case
The Customer Export. A departing sales manager's workstation pulled a full customer export from the CRM. Find out where it went.

Practice, about 80 min · Up to 20 questions · Tools: Browser History Viewer, DB Browser for SQLite, LECmd, Registry Explorer, Thunderbird

Reading
SP 800-86 section 3.4 (reporting). Review the browser and LNK sections of the poster.

Before the lab
Review the browser and LNK sections of the SANS poster.

Deliverable
Lab 8 answers and a short paragraph proving which file left and when, citing three artifacts.

Instructor note
This is the first lab where no single artifact answers the question; grade the paragraph on correlation, not length.

Week 10: Memory forensics

Objectives
• Run Volatility 3 process, network and DLL plugins.

• Identify the suspicious process.

Case
First Look: What's in Memory. One memory capture. Find the process that shouldn't be running, where it lives, and the server it phones home to.

Practice, about 37 min · Up to 15 questions · Tools: Volatility, text editor

Reading
Volatility 3 docs: getting started, pslist, pstree, netscan, dlllist.

Before the lab
Install Volatility 3 and run windows.info against the memory image in the lab pack while online, so it caches the Windows symbols. 16 GB of RAM recommended.

Deliverable
Lab 9 answers.

Instructor note
Budget time for install problems. Pair students with working installs with those without.

Week 11: Code injection in memory

Objectives

• Find injected and unlinked modules.

• Tie a memory finding to disk and network artifacts.

Case

Injected Code in Memory. A workstation called a flagged address and nothing showed up on disk. Work its memory image, disk image and packet capture to find what was running, what it loaded, and where it called.

Practice, about 119 min · Up to 20 questions · Tools: Volatility, The Sleuth Kit, Wireshark, text editor

Reading

Volatility 3 docs: malfind, ldrmodules. One vendor write-up on process injection of your choosing.

Before the lab

Read the Volatility 3 pages for malfind and ldrmodules.

Deliverable

Lab 10 answers and the one memory finding tied to a disk or network artifact.

Instructor note

Hard case; set expectations that a partial but well-evidenced answer scores.

Week 12: Network forensics

Objectives

• Read a PCAP in Wireshark.

• Extract hosts, sessions and a transferred file.

Case

First Look: Reading a Packet Capture. One packet capture from a workstation that looked compromised. Work out what it looked up, what it kept contacting, where it logged in, and what it sent.

Practice, about 33 min · Up to 15 questions · Tools: Wireshark, tshark

Reading

Wireshark User's Guide chapters 3 (capturing) and 6 (display filters); Follow TCP Stream.

Before the lab

Install Wireshark. Work the three built-in capture tutorials.

Deliverable

Lab 11 answers and the number of bytes pushed out over FTP, with the stream that shows it.

Instructor note

Display filters are the whole skill; demonstrate five before the lab.

Week 13: Mobile forensics

Objectives
• Query an Android mmssms.db and recover deleted rows from unallocated pages.

• Convert millisecond Unix timestamps.

Case
The Texts They Deleted. An employee deleted texts before handing in a company phone. Get back what was deleted and work out who it was with.

Practice, about 70 min · Up to 15 questions · Tools: DB Browser for SQLite, ALEAPP, Autopsy

Reading
SP 800-101r1 sections 3 and 4 (mobile data stores and extraction levels). SQLite file format documentation: the freelist.

Before the lab
Read the SQLite file format page on the freelist, and practice converting millisecond Unix timestamps.

Deliverable
Lab 12 answers.

Instructor note
Deleted-row recovery is the highlight; have students show the freelist record, not only the answer.

Week 14: Capstone practical and report

Objectives
• Work a multi-host intrusion end to end.

• Deliver an investigation report with chain of custody.

Case
Credential Theft and Lateral Movement. A service account turned up on servers it never touches. Work out from one workstation's logs, memory and a capture how it was taken and where it went.

Timed exam, 120 min, with report · Up to 20 questions · Tools: Volatility, EvtxECmd, Wireshark, Registry Explorer, Event Viewer

Reading
Re-read SP 800-86 section 3.4 and the NIJ chapter on reporting; the rubric in section 8.

Before the lab
Review the report rubric and the investigation report template that comes with the capstone lab. Prepare a custody form in advance.

Deliverable
Capstone submitted in the portal within 120 minutes; investigation report due one week later.

Instructor note
Run as a timed exam with the investigation report added; the report is written afterwards from the student's own saved answers.

8. Report rubric

Applied to the written report that follows the final timed assessment. The report is written from the student's own saved answers for their own variant, so two reports in the same class never describe the same facts.

Criterion	Weight	Full credit looks like
Findings	40%	Each finding states what happened, when, and which account or device did it, and is correct for the student's own variant.
Evidence	25%	Every finding cites the artifact, the record and the tool used; hashes and paths are exact.
Method	15%	The steps could be repeated by another examiner from the report alone; assumptions are stated.
Timeline	10%	Events are in one normalized timezone, in order, with sources.
Writing	10%	Executive summary first; plain language; no speculation presented as fact.

9. Running the course in Red Herrings

1. Open Courses, pick this course, enter the class size or import the roster CSV, and press Generate the whole course. One job per week is created with the mode and time limit in the schedule.

2. Each week, open that week's job and hand out the student ZIPs or the private portal links. Portal links can be exported as a CSV for the LMS.

3. Timed weeks run in exam mode with integrity logging. Release scores from the job page after the sitting.

4. Grade from the job page or the Grading screen; export to Canvas, Blackboard, Moodle, D2L or QTI, or let LTI pass grades back.

5. Term Analytics shows the whole course at the end of term: scores by week, the questions most often missed, and integrity events.

Syllabus text, policies and the rubric may be copied into institutional templates without attribution.